Deutscher Bundestag
14. Wahlperiode

Drucksache 14/850

04. 05. 99

Sachgebiet 204

Unterrichtung

durch den Bundesbeauftragten für den Datenschutz

Tätigkeitsbericht 1997 und 1998 des Bundesbeauftragten für den Datenschutz – 17. Tätigkeitsbericht –

Gliederung

Zugeleitet mit Schreiben des Bundesbeauftragten für den Datenschutz vom 4. Mai 1999 gemäß § 26 Abs. 1 des Bundesdatenschutzgesetzes.

Abbildungsverzeichnis

1 Einführung
– Überblick und Ausblick –

Dieser 17. Tätigkeitsbericht, den ich dem Deutschen Bundestag vorlege, gibt einen Überblick über die Schwerpunkte meiner Arbeit in den Jahren 1997 und 1998. Zugleich weist der Bericht auf Fragen und Probleme beim Datenschutz hin, die in der nahen Zukunft dringend einer Antwort bedürfen. Er ist der dritte in meiner Amtszeit als Bundesbeauftragter für den Datenschutz. In dem Berichtszeitraum bin ich vom Deutschen Bundestag in das Amt des Bundesbeauftragten für den Datenschutz mit großer Stimmenmehrheit wiedergewählt worden. Den Mitgliedern des Deutschen Bundestages danke ich nicht nur für diesen großen Vertrauensbeweis, sondern auch für die fortwährende, vielfache Unterstützung und Aufgeschlossenheit für meine Aufgaben. Den Mitarbeiterinnen und Mitarbeitern meiner Dienststelle danke ich vor allem für zuverlässige und engagierte Zusammenarbeit. Insbesondere die vielen, an mein Haus gerichteten Bürgereingaben sind eindrucksvoller Beweis dafür, daß das Amt des Bundesbeauftragten als Anwalt des Bürgers in Sachen Datenschutz auch aufgrund seiner Unabhängigkeit längst breite Akzeptanz in der Bevölkerung gefunden hat.

Auch in meiner zweiten und letzten Amtsperiode will ich mich unter Ausgleich der widerstreitenden Interessen engagiert für das Persönlichkeitsrecht der Bürgerinnen und Bürger einsetzen und dem Parlament und der Regierung mit Rat zur Seite stehen. Datenschutz muß dem Schutz des allgemeinen Persönlichkeitsrechts ebenso genügen wie dem Anspruch der Allgemeinheit auf erforderliche Informationen. Auch in der Zukunft werden daher Kompromisse nicht selten unvermeidlich sein; wie überhaupt in datenschutzrechtlichen Streitfragen häufig das Persönlichkeitsrecht mehr erfolgreich beeinflussen kann, wer vertretbar Kompromißbereitschaft zeigt und nicht einseitig auf festgefahrener Auffassung beharrt.

1.1 Die neue Phase des Informationszeitalters

Die neue Phase des Informationszeitalters mit ihren bahnbrechenden Technikinnovationen ist unübersehbar. Während die sechziger und siebziger Jahre die Zeit der zentralen und großen Informationssysteme waren, kamen in den achtziger Jahren die Personalcomputer dazu, und die neunziger Jahre sind die Zeit der Vernetzung der Systeme. Die Telekommunikationsnetze sind gigantisch gewachsen. Diese technologischen Schritte ermöglichten einen völlig neuen Umgang mit personenbezogenen Daten. Nicht nur die Menge der Daten, sondern auch deren Kombinierbarkeit und die Verwertbarkeit der Daten, die bei der Nutzung der Informationstechnologie anfallen, stellen eine neue Herausforderung für den Datenschutz dar. Diese Entwicklung hat sich in atemberaubendem Tempo vollzogen. Während für die Einführung des Radios noch 38 Jahre ins Land gingen, bevor ihm 50 Millionen Menschen zuhörten, waren es beim Fernsehen lediglich 13 Jahre und beim Internet nur noch vier. Kein anderes Medium breitet sich so schnell aus wie das Internet. In den USA wächst die Informationsbranche doppelt so schnell wie die Volkswirtschaft insgesamt. Nach Angaben des US-Handelsministeriums verdoppelt sich der Datenverkehr im Internet alle 100 Tage. Nach neuesten Schätzungen wird der Handel per Internet in Deutschland in zwei Jahren ein Volumen von 25 Mrd. DM haben, vor einem Jahr lag dieser noch bei 3,7 Mrd. DM.

Die „Schöne Neue Welt“ zwischen Multimedia und Internet stellt nach Expertenmeinung den gewaltigsten Sprung in der Geschichte der Kommunikation seit der Erfindung des Buchdrucks dar. Die noch vor wenigen Jahren unter den Deutschen eher vorwiegende Skepsis gegenüber dieser technischen Neuerung hat sich inzwischen gewandelt. Für die Jüngeren in unserer Gesellschaft hat dies bereits ein ganz anderes Geldausgabeverhalten zur Folge. Nach Auswertungen eines Kreditinstituts stecken die 20- bis 35jährigen Kunden bereits ein Drittel ihrer monatlichen regelmäßigen Ausgaben in die modernen Kommunikationstechniken und -services, was früher in dieser Höhe den Ausgaben für Miete und Wohnen vorbehalten war. Längst hat sich hierauf der Markt eingestellt. Dienste wie E-Mail oder World-Wide-Web sind nicht mehr nur Spielwiese von Technikfreaks oder Wissenschaftlern (s. auch Nr. 8).

1.2 „Big Brother“ im 21. Jahrhundert? – Dringender Handlungsbedarf für mehr Datenschutz auf dem privaten Sektor

Ohne Frage haben die Technologien der Informationsgesellschaft unseren privaten und beruflichen Alltag erleichtert und bereichert. Noch nie war es aber so leicht wie heute, die persönlichen Daten der Bürgerinnen und Bürger zu nutzen.

Besteht dadurch die Gefahr, daß unser Alltag entprivatisiert wird?

Droht die Privatsphäre im Informationszeitalter gar zu verschwinden?

Welchen, unter Umständen hohen Preis muß der Bürger für den Informationskomfort zahlen?

Ist bei dieser schnellen und weltweiten Entwicklung noch für Datenschutz und Sicherheit gesorgt?

Immer mehr stellt sich die Frage, ob die Datenschutzkonzepte aus den siebziger und achtziger Jahren den neuen Entwicklungen standhalten können. So sicher wie man in der Regel bei der Nutzung des Internets Datenspuren hinterläßt, so sicher entstand durch die technischen Möglichkeiten der Wunsch von potentiellen Kunden möglichst viel zu wissen und die Daten über die verschiedensten Lebensbereiche mit dem Ziel zusammenzuführen, den Menschen für die eigenen – lauteren oder unlauteren – Zwecke transparent zu machen.

Als der Umfang der Fragen zur Volkszählung 1983 bekannt wurde, bewegte die Bürgerinnen und Bürger die Frage, ob sich Deutschland zu einem Überwachungsstaat zu verändern drohte. Viel Mißtrauen erhob sich aus

Sorge um einen allmächtigen Big Brother. Zurückblickend waren diese Sorgen unbegründet. Das Datenschutz-Szenario hat sich in diesen 16 Jahren jedoch grundlegend geändert. Der moderne Mensch spaltet sich auf in viele virtuelle Existenzen. Insofern gibt es keinen allmächtigen Big Brother, eher beobachten ihn aber viele kleinere Brüder sehr aufmerksam von der Seite. Nach einer Untersuchung ist jeder Deutsche über 18 Jahre allein 52mal in Unternehmensdatenbanken gespeichert. Dazu kommen der öffentliche und der nicht kommerzielle Bereich. 90 % aller Informationen schlummern hiernach noch ungenutzt in den Speichern. Schon werden Analyseinstrumente immer weiter ausgefeilt, um daraus individuelle Profile herzustellen. Eines der Schlagworte der Wirtschaft im Informationszeitalter heißt daher Data-Mining. Damit sollen Kundenpotentiale optimal ausgeschöpft werden. Diese neuen Analysemethoden sind aber nicht nur für das Marketing geeignet. Sie ebnen auch den Weg zum Gläsernen Kunden (s. auch Nr. 8.2.4).

1.2.1 Ist der gläserne Konsument nur eine Utopie?

Im Unterschied zu der Situation im Zusammenhang mit der Volkszählung 1983 empfinden Bürgerinnen und Bürger eine Bedrohung ihrer Persönlichkeitsrechte heutzutage weniger durch staatliche Stellen als durch die wachsende Technisierung ihrer Umwelt und die damit verbundenen Eingriffe nicht-öffentlicher Stellen in ihre Privatsphäre. Umfangreiche, freikäufliche Datensammlungen auf CD-ROM sowie die zunehmende Bedeutung des Adreßhandels und der Direktwerbung sind dafür nur einige Beispiele. Immer wieder macht sich vereinzelt Unbehagen gegen ungefragte Vereinnahmung breit. Genau genommen müßten die seit einigen Jahren durch Deutschland rollenden Befragungswellen alle Kritiker von einst auf die Barrikaden treiben. Ein Beispiel hierfür sind die sogenannten Haushaltsbefragungen, mit denen Bürger detailliert nach ihren Lebensumständen und Konsumgewohnheiten gefragt werden. Wo das durch das Bundesverfassungsgericht eingeschränkte Volkszählungsgesetz nur 15 Fragen zur Wohnsituation zuließ, sind die Haushaltsbefragungen durch private Unternehmen ungleich wißbegieriger. Mit in die Tiefe gehenden Fragen erkunden sie das Wohnumfeld, u. a. auch den evtl. vorhandenen Whirlpool, fragen nebenbei nach der Hausratversicherung oder nach dem Zustand des Gartens. Wie selbstverständlich wird auch die Höhe des monatlichen Nettoeinkommens und der Telefonrechnung abgefragt. Auch wenn privaten Unternehmen die Möglichkeit fehlt, Bürger zur Beantwortung von Fragen zu verpflichten, sind privat durchgeführte Haushaltsbefragungen unter datenschutzrechtlichen Aspekten eher brisant. Ich jedenfalls sehe diese datenschutzrechtlich als sehr problematisch. Denn der private Bereich ist hinsichtlich der näheren Gestaltung der Umfragen sowie der weiteren Verwendung der erhaltenen Daten kaum rechtlich geregelt. Den Unternehmen stehen damit große Handlungsspielräume zur Verfügung, die sie für ihre Geschäftszwecke nutzen. Um die Betroffenen zur Einwilligung zu bewegen, werden ihnen attraktive Gewinne in Aussicht gestellt. Um den Befragten vollends zu überzeugen, werden Formulierungen gewählt, die es ihm schwer machen, sich auch der Nachteile und Risiken bewußt zu werden. Insgesamt bleibt hier zumindest ein schlechter Nachgeschmack dann, wenn wegen der Art der abgefragten Daten und der Art ihrer Auswertung und Verbreitung doch zweifelhaft bleibt, ob die Betroffenen alle Risiken kennen und richtig einschätzen können (s. Nr. 31.1).

In einer anderen, von der Öffentlichkeit kaum beachteten Aktion schickte ein großes deutsches Direktmarketing-Unternehmen in den Jahren 1992 bis 1994 über 1000 nebenberufliche Mitarbeiter durch Deutschland, die von Straße zu Straße zogen, um jedes Haus zu taxieren: Von Ein-, Zwei-, oder Mehrfamilienhaus, über Reihen- oder Wohnhochhaus usw., über Ortskern oder Ortsrand, über Neben- oder Anwohnerstraße, über Altersklasse und Garten bis zur Benotung von 1 bis 6 für Wohnlage, Gestaltung, Bauweise und Zustand.

Gegenwärtig läuft ein neues Projekt, bei dem eine Gebäude-Bild-Datenbank aufgebaut wird, die nach Fertigstellung fast alle Gebäude im gesamten Bundesgebiet erfassen soll. Die Aufnahmen der einzelnen Gebäude werden ohne Wissen und ausdrückliche Einwilligung der betroffenen Hauseigentümer gefertigt, wobei die Verwendung des Datenmaterials nicht eingegrenzt ist.

Die Beispiele könnten beliebig fortgesetzt werden. Die denkbaren Auswirkungen dieser Entwicklung sind gravierend. Immerhin sind Erkenntnisse zu gewinnen, die einen Menschen womöglich genauer beschreiben, als er sich selbst zu kennen glaubt. Das bisherige Datenschutz-Instrumentarium jedenfalls reicht für diese Entwicklung nicht aus. Es wurde zu einer Zeit geschaffen, als die Leistungsstärke der neuen Systeme noch nicht wirklich begriffen wurde. Zum Schutz der Privatsphäre gehört im Kern, daß jeder Mensch selbst darüber bestimmen kann, wer was wann bei welcher Gelegenheit über ihn weiß. Eine verfassungsrechtliche Grenze ist das Verbot, teilweise oder vollständige Persönlichkeitsprofile zu erstellen, es sei denn, der Bürger ist ausreichend informiert und hat dem zugestimmt. Dieses Verbot wird in Frage gestellt, wenn immer mehr verknüpfbare personenbezogene Informationen verfügbar sind. Hier muß der Gesetzgeber klare Grenzen aufzeigen, damit die schutzwürdigen Belange der Bürgerinnen und Bürger ausreichend zur Geltung kommen.

1.2.2 Keine Rechtsklarheit und Transparenz beim elektronischen Beäugen

Die Videoüberwachung im nicht-öffentlichen Bereich hat in den letzten Jahren weiter rasant zugenommen. Während die Videoüberwachung für staatliche Zwecke in den Polizeigesetzen von Bund und Ländern, aber auch in der Strafprozeßordnung, detailliert geregelt wird (z. B. § 27 BGSG sowie § 100c StPO), besteht nach wie vor keine Rechtsklarheit darüber, unter welchen Voraussetzungen Videoüberwachung durch private Stellen zulässig ist. Auch der Deutsche Bundestag hat in der 13. Wahlperiode die Bundesregierung zu einer gesetzlichen Klarstellung aufgefordert.

Videoüberwachungen können sehr unterschiedlichen – auch guten – Zwecken dienen, z. B. der Kontrolle von

Kasseneingängen, der Einlaßkontrolle von Nebeneingängen, der Sicherung von Personen vor Überfällen oder Unfällen, der Sicherung von Geld und Sachwerten. Damit müssen aber in jedem Einzelfall unterschiedliche verfassungrechtlich geschützte Güter wie Leben, Gesundheit oder Eigentum mit dem ebenfalls geschützten Grundrecht auf informationelle Selbstbestimmung in Einklang gebracht werden. Sicherlich ist Videoüberwachung in Deutschland noch nicht so allgegenwärtig wie in einigen anderen Ländern, z. B. in Großbritannien. Dort nutzen bereits rd. 120 Städte größere Überwachungsanlagen im öffentlichen Bereich. Wenn auch von einer vergleichbar dichten Videoüberwachung in Deutschland noch keine Rede sein kann, zeichnet sich auch hier eine Tendenz zu einer wachsenden Videoüberwachung insbesondere innerstädtischer Bereiche durch Polizei und private Betreiber ab, an die man sich wohl oder übel gewöhnen muß. Immer mehr Bereiche werden davon betroffen sein. So werden z. B. die großen Bahnhöfe von der DB AG mit Video-Anlagen ausgerüstet, die über ferngesteuerte, moderne Überwachungskameras verfügen, die sich automatisch auf die unterschiedlichen Lichtsituationen bei Tag und Nacht einstellen und weite Bereiche der Bahnhöfe erfassen (s. 16. TB Nr. 12.4). Der öffentliche Verkehrsraum in der Umgebung z. B. des Leipziger Hauptbahnhofes urde von der sächsischen Polizei – im Rahmen eines Probelaufes – überwacht. Hinzu kommt die Videoüberwachung durch Geschäftsleute in kriminalitätsbelasteten Innenstadtbereichen.

Danach könnte ein beliebiges Videoüberwachungs-Szenario heute etwa wie folgt aussehen:

Ein völlig harmloser Zugreisender, der in einem Großstadtbahnhof nichts ahnend aus dem Zug steigt, wird durch die Kameras des bahneigenen Videosystems aufgenommen, was auch von den Beamten der nächsten Bahnpolizeiwache beobachtet werden kann. Beim Verlassen des Bahnhofs gerät der Reisende in den Sichtbereich der Videokameras der Landespolizei, die ihn dann in der benachbarten Einkaufszone unbemerkt im Blick behält. Die Videokamera des Bankautomaten hält als nächstes sein Bild fest, und so ließe sich die Geschichte einer Beobachtung durch Videokameras fortsetzen.

Das Problem an der Videoüberwachung ist nicht nur, daß unbescholtene Personen in ihr Visier geraten, sondern sind auch die immensen Mengen von Aufnahmen. Bereits im 16. TB (Nrn. 1.4 und 31.1) habe ich daher auf den dringenden datenschutzrechtlichen Regelungsbedarf zum Einsatz von Maßnahmen der Videoüberwachung hingewiesen. Solche Datenschutzvorschriften stehen immer noch aus. Deshalb wiederhole ich meine Forderung, Rechtsklarheit darüber herzustellen, unter welchen Voraussetzungen Videoüberwachungen zulässig sind. Die anstehenden Regelungen müssen sich an den Zielen maximaler Transparenz und eines angemessenen Schutzes unbescholtener Personen messen lassen. Dringend notwendig ist insbesondere eine Regelung der Fälle, in denen die Bürger ausdrücklich auf die Videoüberwachung z. B. in Geschäftsräumen hingewiesen werden müssen. Ferner ist zu regeln, für welche Zwecke die Aufnahmen benutzt werden dürfen. In diesem Zusammenhang sollte ferner geprüft werden, ob unbefugte Videoüberwachung künftig – jedenfalls in besonders schweren Fällen – unter Strafandrohung zu stellen ist.

1.2.3 Internet: Kommunikation mit neuen Risiken

Ein immer größer werdender Teil unserer Kommunikation läuft elektronisch über weltweite Datennetze ab. Das Internet ist damit das Kommunikationsmedium der Zukunft. Es stellt für den Verbraucher eine Fülle von Informationen und Diensten bereit, die ein breites Spektrum von reinen Informationsdatenbanken über Online-Banking bis hin zu elektronischem Handel umfassen. Viele Produkte – von Flugreisen über verschiedene Arten von Dienstleistungen bis hin zu Büchern – können über das Internet geordert werden. Für den Verbraucher und den Schutz seiner Daten ergeben sich daraus neue Probleme. Kauft man heute z. B. konventionell irgendwelche Produkte, so zahlt man bar und nimmt die Ware mit. Später wissen dann weder der Verkäufer noch die kontoführende Bank, wer welche Waren gekauft hat und wieviel diese gekostet haben. Niemand kontrolliert, für welche Produkte man sich während des Einkaufsbummels interessiert und welche Auslagen man wie lange angeschaut hat. Im Internet ist das anders. Bereits beim Schaufensterbummel hinterläßt jeder Nutzer hier Datenspuren, die vom Anbieter automatisch aufgezeichnet werden können.

Die Kehrseite des neuen Kommunikationsmediums Internet zeigen daher Berichte, die das Netz als chaotisches und unbeherrschbares System beschreiben, in dem es weder Datenschutz noch Datensicherheit gibt. Ein Grund dafür ist, daß zur Datenübertragung im Internet weder der Absender noch der Empfänger den Weg hierzu vorgeben können. Durch das – technisch bedingte – Zwischenspeichern der Daten in jedem der Knoten, die an einer Übertragung beteiligt sind, ist der Betreiber des Knotens theoretisch in der Lage, die Datenpakete zu nutzen, statt sie – wie in Deutschland vorgeschrieben – unverzüglich zu löschen. Da jeder Knotenbetreiber die Daten infolge seiner Mitwirkung an der Übertragung nutzen könnte, ist das Risiko einer offenen Übermittlung und damit einer ungewollten Verbreitung der Daten im Internet unkalkulierbar. Ein wirksamer Schutz gegen das Mitlesen der Daten durch Unbefugte ist durch die Verwendung von Verschlüsselung möglich (s. auch Nrn. 8.4, 8.7 und 8.10).

Angesichts der zunehmenden Bedeutung der internationalen Datennetze und der damit verbundenen Risiken für die Privatsphäre der Nutzer sind weltweit verbindliche gesetzliche Regelungen erforderlich. Erste Schritte in diese Richtung hat die OECD unternommen, die in ihrem Schlußdokument zur Ottawa-Konferenz vom Oktober 1998 das Ziel des Schutzes der Privatsphäre in weltweiten Datennetzen unterstreicht. Vorerst wird jedoch auf Selbstregulierung gesetzt. So sollen sich z. B. US-Firmen auf freiwilliger Basis einem Datenschutz-Verhaltenscodex unterwerfen. Die gesetzlichen Regelungen sind weltweit unterschiedlich. Zum Teil fehlen sie, und bisweilen werden selbst die geltenden Gesetze durch die Diensteanbieter nur nachlässig umgesetzt. Der Nutzer hat also allen Anlaß, selbst vorsichtig zu sein.

Bevor er seine persönlichen Daten Preis gibt, sollte er prüfen, ob dies für die angebotene Leistung tatsächlich notwendig ist. Jeder Nutzer sollte also abwägen, ob für ihn persönlich das „Preis-Leistungsverhältnis“ stimmt, was heißt, ob er bereit ist, für eine bestimmte Ware oder Dienstleistung Teile seiner Privatsphäre aufzugeben, und zwar oft weltweit und auf Dauer (s. auch Nrn. 8.2.4 und 8.4).

1.2.4 Boom der privaten Sicherheitsbranche: Datenschutz in der Rand- oder Grauzone?

Private Sicherheitsdienste haben in den vergangenen Jahren zunehmend Aufgaben übernommen, darunter auch Aufgaben, die – jedenfalls nach dem Verständnis vieler Bürgerinnen und Bürger – eigentlich von der Polizei wahrgenommen werden sollten. Wurden früher mit privaten Sicherheitsdiensten in der Regel Wachdienste verbunden und vielleicht noch Detekteien, kommen heute vor allem „Schwarze Sheriffs“ oder „Bodyguards“ dazu.

Die Sicherheitsdienste erfahren über ihre Kunden und über diejenigen, die sie bewachen oder beobachten sollen, viel. In das Visier der privaten „Hilfssheriffs“ kommen aber nicht nur bescholtene, sondern auch unbescholtene Bürger. Dossiers über Personen, Warndateien oder verdeckte Ermittlungen und Observationen sind Stichworte, die ein Licht auf die Datenschutzproblematik der wachsenden Sicherheitsbranche werfen. Wie die Sicherheitsdienste diese Daten erheben oder verbreiten, ist nicht speziell geregelt. Hier gelten bislang lediglich die Vorschriften des Bundesdatenschutzgesetzes. Dessen Regelungen sind aber zu allgemein, um das Persönlichkeitsrecht von Betroffenen angesichts der besonderen Risiken der Sicherheitsbranche zu schützen. Wenn z. B. ein privater Sicherheitsdienst, der Bodyguards stellt, zur Aufklärung des Umfeldes der zu schützenden Person alle möglichen Daten über Verwandte, Freunde, Nachbarn oder Bekannte sammelt, evtl. Fotos oder Videos fertigt, tut er dies zur Erfüllung seines Sicherungsvertrages. Die Betroffenen erfahren in der Regel nichts davon und können damit u. a. ihren Auskunfts- oder Löschungsanspruch nicht geltend machen. Und auch im Hinblick auf das staatliche Gewaltmonopol ist zu klären, welche Daten private Sicherheitsdienste erheben dürfen, in welcher Form und zu welchem Zweck dies möglich sein soll, an wen die Daten weitergegeben werden dürfen und wann sie zu löschen sind.

Besonders problematisch wirken sich diese rechtlichen Defizite aus, wenn private Sicherheitsdienste mit der Polizei zusammenarbeiten bzw. ihr Material zur Verfügung stellen. Die Polizei hat präzise rechtliche Vorgaben für den Umgang mit personenbezogenen Daten. So darf sie nur bei Verdacht auf bestimmte Straftaten – aufgrund einer richterlichen Anordnung – ein Telefon überwachen, Videoaufnahmen fertigen oder ein Haus durchsuchen. Ein privater Sicherheitsdienst entscheidet über den Einsatz seiner Mittel nach mehr oder weniger eigenem Gutdünken. Die Polizei darf ihr gewonnenes Material nur nach den Vorgaben der Strafprozeßordnung oder der Polizeigesetze verwenden und hat es nach vorgegebenen Fristen, die auch kontrolliert werden, zu löschen. Der private Sicherheitsdienst hat dagegen einen großen Spielraum.

Im März 1997 fand auf Beschluß des Innenausschusses des Deutschen Bundestages eine öffentliche Anhörung zur Notwendigkeit gesetzlicher Regelungen für private Sicherheitsdienste statt. Leider wurde kein Regelungsbedarf hinsichtlich der Erhebung, Verarbeitung oder Übermittlung von Daten durch private Sicherheitsdienste gesehen. Als wünschenswert wurde lediglich angesehen, das Niveau der Sachkunde – u. a. auch wegen des zulässigen möglichen Waffengebrauchs durch die Sicherheitsbranche – anzuheben.

Mit Blick auf das unveränderte Wachstum dieser Branche hoffe ich, daß im Zusammenhang mit der ohnehin notwendigen Novellierung des Datenschutzrechts hier Regelungen geschaffen werden. Die betroffenen Bürger haben sonst wenig Möglichkeiten, ihren Anspruch auf den Schutz ihres Persönlichkeitsrechts durchzusetzen, wenn sie z. B. als Besucher einer Firma, als Personal einer bewachten und gesicherten Einrichtung oder als zufälliger Bekannter einer beobachteten Person in das Visier der „Hilfssheriffs“ geraten (s. Nr. 2.1.2.1).

1.3 Datenschutz in der Einstellung der Bürger: Appell zu mehr eigenverantwortlichem Datenschutz

Eine im vergangenem Jahr von den Datenschutzbeauftragten des Bundes und der Länder veranlaßte Repräsentativbefragung läßt auf großes Mißtrauen gegenüber Institutionen im Hinblick auf den zulässigen Umgang mit privaten Daten schließen.

Ein Drittel der Befragten gab an, daß nach ihrem Eindruck ihre persönlichen Daten einmal oder mehrmals widerrechtlich gegen ihren Willen verwendet worden seien. Bundesweit erklärten zwei Drittel, daß sie sich dadurch sehr stark oder mittelstark persönlich beeinträchtigt fühlen. Das Ergebnis sehe ich insgesamt als deutliches Signal auch an die Politik, den Datenschutz zu stärken.

Ohne Zweifel hat sich das Bewußtsein der Bürgerinnen und Bürger hinsichtlich des Umgangs mit ihren Daten durch Dritte grundlegend geändert. Dies belegt auch die große Zahl von Beschwerdeschreiben an mein Haus z. B. zum Thema Adreßhandel und Direktmarketing. Typische Schreiben hierzu lauten etwa: „Vor einiger Zeit erhielt mein Sohn ein Schreiben der Versicherung xyz. Er wurde dabei u. a. auf die Unfallversicherung angesprochen und man hoffte, daß er auch einen Ausbildungsplatz gefunden habe.“ Viele Einsender fragen, auf welchem Wege ein Unternehmen bestimmte, auch besonders schutzwürdige Daten erhalten hat und wenden sich gegen die häufig nichtssagenden Antworten der Unternehmen. Sie nehmen hierbei ihre selbstverständlichen Datenschutzrechte, wie z. B. Auskunft oder Löschung, in Anspruch.

Vielfach sind aber für Datenschutzverstöße auch Sorglosigkeit und Unwissenheit der Betroffenen im Umgang mit den eigenen Daten verantwortlich zu machen. Typi-

scherweise lauten Schreiben in diesen Fällen etwa: „Vor einigen Jahren habe ich eine Messe über .... in .... besucht. Dort habe ich an einer Verlosung teilgenommen. Für den Gewinnfall mußte ich meine Adresse angeben.“ Vielleicht warten einige der Betroffenen heute noch vergeblich auf ihre Gewinne; auffällig ist jedenfalls, wie leichtfertig oder gar leichtsinnig gelegentlich mit eigenen Daten umgegangen wird. Diese Kehrseite beim Umgang mit der eigenen Privatsphäre ist z. B. tagtäglich auch auf öffentlichen Plätzen oder in öffentlichen Verkehrsmitteln zu beobachten, wenn Nutzer von Handies sich äußerst freizügig und laut über ihr Privatleben auslassen. Dies muß für Dritte nicht nur lästig sein, es kann auch Neugier erwecken.

Insbesondere was die freiwillige Weitergabe ureigener Daten an private Dritte betrifft, muß jeder einzelne Verantwortung für den Schutz seiner Daten aktiv übernehmen. Hier appelliere ich an die Bürgerinnen und Bürgern zu mehr eigenverantwortlichem Datenschutz. Dazu gehört, mehr darauf zu achten, wem man welche Informationen und Auskünfte gibt. Dazu gehört aber auch, informiert darüber zu sein, was mit den Daten überhaupt geschieht. Für Informationen über den Datenschutz wie auch für die Durchsetzung ihrer Datenschutzrechte stehen den Bürgerinnen und Bürgern die Datenschutzbeauftragten von Bund und Ländern wie auch die Aufsichtsbehörden der Länder zu Seite. Wer seine Rechte nicht kennt, kann sie auch nicht in Anspruch nehmen.

1.4 Datenschutz 2000: Stillstand oder Renaissance?

Der Datenschutz steht an einem Wendepunkt. Dies zeigen nicht nur intensive Diskussionen in Fachkreisen und Tagungen bis hin zum Deutschen Juristentag 1998, sondern auch in der breiten Öffentlichkeit. Knapp 16 Jahre nach dem Volkszählungsurteil des Bundesverfassungsgerichts schlägt sich das Datenschutzrecht in einer kaum noch überschaubaren Menge von bereichsspezifischen Vorschriften nieder. Mag auch für einen Teil dieser Vorschriften der Grund im Volkszählungsurteil zu suchen sein, wonach der Eingriff in das Persönlichkeitsrecht detailliert zu regeln ist, so haben viele dieser neuen bereichsspezifischen Vorschriften lediglich alte Übungen und neue Begierden gesetzlich abgesichert. Wenn es auch nachvollziehbar ist, die neuen technischen Möglichkeiten der Datenverarbeitung weitgehend zu nutzen, so ist darüber nicht immer die Zielvorgabe des Bundesverfassungsgerichtes beachtet worden, das verfassungsrechtlich verankerte Grundrecht auf informationelle Selbstbestimmung weiter zu stärken. Herausgekommen ist vielfach ein Paragraphendschungel, der auch vom Fachmann kaum noch zu überschauen ist. Im gleichen Maße hat das Bundesdatenschutzgesetz als Auffang- und Querschnittsgesetz an Bedeutung verloren. Tatsache ist, daß es den Technologiesprüngen bei der Informationsverarbeitung im privaten Bereich nicht Rechnung trägt. Hier sieht das Gesetz nur allgemein Abwägungen vor, wobei die formelhafte Berücksichtigung der schutzwürdigen Interessen der Betroffenen nicht viel mehr als schemenhafte Bedeutung hat. Angesichts steigender Datenmacht in privater Hand sind hier dagegen klare Grenzlinien gefordert.

Auch mit Blick auf diese ungeschminkte Beschreibung der Datenschutzsituation in Deutschland sehe ich keinen Grund, der Schwarzweißmalerei das Wort zu reden oder in Pessimismus zu verfallen. Keineswegs kann die Vergangenheit des Datenschutzes so beschrieben werden: „Sie wollten Datenschutz und bekamen Gesetze.“ Das Fazit muß vielmehr sein: Die Erneuerung des Datenschutzes ist notwendig, und sie muß jetzt angepackt werden. Das Eckwerte-Papier der SPD-Fraktion sowie der Entwurf der Fraktion Bündnis 90/Die Grünen zur Novellierung des Bundesdatenschutzgesetzes bieten hierzu vielversprechende Ansätze. Angesichts des rasanten Tempos der Entwicklung in eine neue Phase der Informationsgesellschaft darf die Erneuerung des Datenschutzes nicht auf die lange Bank geschoben werden.

Die Kernanliegen des Datenschutzes – die Selbstbestimmtheit des einzelnen und die Transparenz des Verwaltungs- oder Wirtschaftshandelns – bleiben weiterhin im Zentrum aller Überlegungen zum Datenschutz. Die Novellierung des Datenschutzes darf sich auch nicht auf die längst fällige Umsetzung der EG-Datenschutzrichtlinie beschränken. Sie darf insbesondere nicht Halt machen vor den längst fälligen Regelungen zu neuen Technologien, wie Verbundverfahren, Chipkarten und Videoüberwachung. Um den neueren Entwicklungen der Informationstechnik und ihren Auswirkungen auf die Privatsphäre gerecht zu werden, müssen vor allem Instrumente für die Gewährleistung eines effektiven Selbstschutzes der Bürgerinnen und Bürger geschaffen werden, wie z. B. Verschlüsselungsverfahren für sensitive Daten, die Einführung eines Datenschutzaudits sowie die Zielvorgaben der Datensparsamkeit, Anonymisierung und Pseudonymisierung. In den neuen Technologien nützt Datenschutz nichts, wenn er nicht technisch umgesetzt werden kann. Deshalb kommt es darauf an, von vorneherein Datenspuren, die sich zu einem Mißbrauch eignen, zu vermeiden. In diesem Sinne begrüße ich die angesprochenen Initiativen aus dem parlamentarischen Raum ausdrücklich. Meine Erwartungen richten sich auf den Deutschen Bundestag, daß er in einem erneuerten Datenschutzrecht die Persönlichkeitsrechte noch deutlicher herausstellt und dem Datenschutz den Platz verschafft, der ihm in der Informationsgesellschaft zu Beginn des neuen Jahrhunderts zukommt (s. auch Nr. 2.1.2).

1.5 Erfolgskontrolle bei besonderen Eingriffsbefugnissen dringender denn je

In der Diskussion um besonders einschneidende strafprozessuale Ermittlungsbefugnisse habe ich mehrfach neue, vertrauensbildende Maßnahmen für eine Stärkung des Persönlichkeitsrechts gefordert. Nach wie vor ist das Wissen über die Wirksamkeit dieser Befugnisse unzureichend. Auch mit Blick auf die im vergangenen Jahr eingeführte akustische Wohnraumüberwachung und die erweiterten Möglichkeiten einer Telefonüberwachung nach § 100a StPO kommt es mehr denn je jetzt darauf an, eine wirksame Erfolgskontrolle in die Praxis umzusetzen.

Allein bei der Telefonüberwachung nimmt Deutschland weiterhin eine Spitzenstellung ein. In 1997 betrug die Anzahl der nach §§ 100a, 100b StPO erfolgten Anordnungen für Telefonüberwachungen 7 776, wovon 3 828 Mobiltelefonanschlüsse betroffen waren (s. BT-Drs. 13/11354).

Nach der Rechtsprechung des Bundesverfassungsgerichts bedarf es einer gründlichen Bestandsaufnahme und Evaluierung des strafprozessualen und polizeirechtlichen Instrumentariums, um einerseits wegen der gebotenen Effizienz und andererseits wegen der Einschränkung von Grundrechten Verdächtiger und erst recht Unbeteiligter das richtige Maß zu finden. Neue Eingriffsbefugnisse müssen deshalb nach ihrer Einführung und Anwendung hinsichtlich ihrer Wirkungen bewertet werden können, um sowohl ein Unter- als auch ein Übermaß zu vermeiden.

Für die Fälle der akustischen Wohnraumüberwachung hat der Gesetzgeber nunmehr erfreulicherweise Berichtspflichten der Staatsanwaltschaft gegenüber der obersten Justizbehörde und der Bundesregierung gegenüber dem Bundestag auferlegt (s. Nr. 6.1).

Entsprechende Berichtspflichten halte ich darüber hinaus auch für den Bereich der Telefonüberwachung und für präventivpolizeiliche Befugnisse wie die verdeckte Datenerhebung für unabdingbar. Hierbei sollten auch Erkenntnisse über die persönliche Einstellung von Richtern, Staatsanwälten und Kriminalbeamten bei der Anwendung dieser Befugnisse untersucht werden, beispielsweise inwieweit die Telefonüberwachung nicht mehr als „ultima ratio“, sondern als bequeme Standardmaßnahme in einem nur etwas komplexeren Ermittlungsverfahren angesehen wird.

Bei einer umfassenden, objektiven, kritischen und zugleich fairen Erfolgskontrolle kann es letztlich keine Gewinner und Verlierer geben, da sie auf das von allen Beteiligten gleichermaßen akzeptierte Ziel eines Freiheit und Sicherheit garantierenden Rechtsstaates gerichtet ist. In diesem Sinne hoffe ich auf baldige Fortschritte und Erfolge bei der im Bundeskriminalamt eingerichteten Rechtstatsachensammelstelle (s. Nr. 11.2).

1.6 Neuer Telekommunikations- und Postdienstmarkt: Datenschutz stärken

Mit der Liberalisierung des Telekommunikations- und Postdienstmarktes wurde mir die Datenschutzkontrolle für Unternehmen übertragen, die Telekommunikationsdienste oder Postdienstleistungen erbringen. Beide Bereiche bilden inzwischen neue Schwerpunkte in meinem Hause, ist doch die Zahl von Unternehmen, die diese Dienste erbringen, in jüngster Zeit stark gewachsen. Mit den Telekommunikationsunternehmen gibt es bereits Gesprächskreise, mit den Postdienstunternehmen wurden die Gespräche aufgenommen. Auch deren Kunden wenden sich inzwischen in einer Vielzahl von Anfragen um Auskunft oder um Unterstützung an mich. Viele Beiträge in diesem Tätigkeitsbericht geben hiervon eindrucksvoll Beispiel (s. Nrn. 10.2, 10.3, 29.2.1, 29.5.1, 29.5.2, 29.7).

Beiden Bereichen ist gemeinsam, daß gute Datenschutzregelungen die Akzeptanz und Verbreitung der einzelnen Dienstleistungen fördern. Im allgemeinen kann auch davon ausgegangen werden, daß die Unternehmensleitungen in den Strategiekonzepten dem Datenschutz das notwendige Gewicht verleihen. Denn der hohe Schutz der Vertraulichkeit der Nachrichten auf dem Telekommunikations- oder Postsektor ist nicht nur eine Forderung des Datenschutzes, sondern deckt auch in vollem Umfang das Verbraucherinteresse.

Gerade bei der Gestaltung neuer TK-Dienstleistungen müssen beide Aspekte berücksichtigt werden. So muß die Möglichkeit einer detailreichen Registrierung des Telekommunikationsvorganges genauso gegeben sein, wie die Möglichkeit der anonymen Kommunikation. Diese Forderung für die Gestaltung neuer TK-Dienstleistungen ist inzwischen in Gesellschaft und Politik allgemein akzeptiert.

Gelegentlich scheint das Prinzip vom „königlichen Kunden“ auf den Kopf gestellt. Ein Beispiel hierfür ist die Datenstruktur der GSM-Telefonnetze (D 1-, D 2- und E-plus-Netz). Bei ihrer Konzeption wurde eine selbst von Experten kaum übersehbare Fülle von Datenspeicherungen vorgesehen, von denen viele bis heute nicht benötigt werden. Maßgebliche Richtschnur war hier wohl eher: mal sehen, vielleicht können wir sie ja noch brauchen. Anonyme oder pseudonyme Nutzungsmöglichkeiten wurden nicht vorgesehen oder erst später „hineingeflickt“. So gibt es bis heute in den Mobilfunknetzen keine Tarife, die tatsächlich von der Entfernung der beiden Kommunikationspartner abhängig sind; gleichwohl wird der Standort des Handy beim Gesprächsbeginn registriert. Auch bei der Telekommunikation müssen datenschutzfreundliche und datenarme Technologien maßgebliche Leitlinien bilden. Sowohl in dem zuständigen Bundesministerium als auch den TK-Unternehmen habe ich hierzu jedoch deutliche Informationslücken festgestellt, wie solche Technologien aussehen könnten. So ist auch erklärlich, daß mögliche Strategien für eine Problemlösung bislang nicht entwickelt wurden (s. Nr. 10.1.8).

Auch im Postbereich haben gelegentlich vorschnelle Vertriebskonzepte zu Lasten des Datenschutzes eher Unbehagen ausgelöst, so z. B. im Herbst 1998, als die Deutsche Post AG verdächtigt wurde, Briefträger als Marketingspione einzusetzen (s. Nr. 29.7).

1.7 Wachsende Datenbestände über Kundendaten: Neue Begehrlichkeiten des Staates bei Auskünften?

Für den Gesetzgeber war es bei der Liberalisierung des Telekommunikations- und Postdienstmarktes ein besonderes Ziel, das Fernmelde- bzw. Postgeheimnis unverändert zu erhalten. Durchbrechungen sollten allenfalls im früheren Umfang erlaubt sein. Ob diese Maxime unverändert ihre Gültigkeit hat, scheint gelegentlich in Frage zu stehen.

Das Telekommunikationsrecht enthält an mehreren Stellen Rechtsgrundlagen für Auskünfte über Kundendaten an Sicherheitsbehörden. So müssen Telekommunikationsunternehmen eine Kundendatei führen, in die

Rufnummern bzw. Rufnummernkontingente sowie Name und Anschrift der Inhaber der Rufnummern bzw. Rufnummernkontingente aufzunehmen sind. Dies gilt auch, soweit die Kunden in öffentlichen Verzeichnissen nicht eingetragen sind. Auf Ersuchen bestimmter Sicherheitsbehörden hat die Regulierungsbehörde für Post- und Telekommunikation die Daten automatisiert abzurufen und an diese Behörden zu übermitteln. Die Vorschrift des hier in Rede stehenden § 90 TKG ist bereits vor ihrem Inkrafttreten heftig diskutiert worden. Inzwischen haben sich Befürchtungen bewahrheitet, daß die Regelung weit über das angestrebte Ziel hinausschießt, da nach ihr jeder verpflichtet ist, der geschäftsmäßig Telekommunikationsdienste anbietet. Nach Feststellungen der Regulierungsbehörde wären von dieser Vorschrift nach derzeitiger Rechtslage ca. 400 000 Unternehmen betroffen. Deshalb soll in einer ersten Ausbauphase zunächst mit 72 Anbietern von Telekommunikationsdiensten begonnen werden. Wann der zahlenmäßig große Bereich derjenigen Unternehmen einbezogen wird, die Telekommunikationsdienste im Sinne früherer Nebenstellenanlagen anbieten, soll noch entschieden werden. Danach ist wohl damit zu rechnen, daß sämtliche Betreiber von Nebenstellenanlagen, die ihre Anschlüsse Dritten geschäftsmäßig zur Verfügung stellen, künftig entsprechende Kundendateien zu führen haben. Ich habe dies vor allem am Beispiel der Krankenhäuser, wo die ärztliche Schweigepflicht durchbrochen würde, und anhand von anderen Bereichen, in denen Berufsgeheimnisse berührt sind, problematisiert und gefordert, zumindest diese vom Geltungsbereich der Regelung auszunehmen.

Ein anderes gravierendes Problem sehe ich darin, daß staatlichen Stellen bei Anfragen nicht nur die Daten der Personen bekannt werden könnten, nach denen sie tatsächlich suchen, sondern auch die Daten Unbeteiligter, nämlich dann, wenn Anfragen mit unvollständigen Rufnummern oder unvollständigen Namen- bzw. Adressangaben gestellt werden. Auch befürchte ich, daß die Praxis über Auskünfte zu Bestandsdaten von Kunden ausufert, wenn hier nicht ein entsprechender gesetzlicher Riegel vorgeschoben wird. Der Auskunftsanspruch muß deshalb streng auf solche Daten beschränkt werden, die einen besonderen Telekommunikationsbezug haben, wie der Name des Anschlußinhabers, der Standort und die Rufnummer des Anschlusses. Die Preisgabe weiterer Daten, wie z. B. der Bankverbindung oder der Zugehörigkeit zu bestimmten gesellschaftlichen Gruppen bei Sondertarifierung, darf den Telekommunikationsunternehmen nicht abverlangt werden.

Wachsende Datenbestände im privaten Bereich, insbesondere die Kommerzialisierung der Profile, erhöhen offenbar auch das Interesse staatlicher Stellen an privaten Datensammlungen. Im Tätigkeitsbericht finden sich weitere Beispiele für eine Zunahme des Wissensdurstes des Staates (s. Nrn. 6.4 und 10.1.5).

1.8 Datenschutzrechtliche Regelungen im Strafverfahren –- eine (un-)endliche Geschichte?

Ausgerechnet im Bereich der Justiz werden besonders schützenswerte personenbezogene Daten nach wie vor ohne ausreichend präzise Rechtsvorschriften erhoben und verarbeitet. Ich halte den jetzigen Rechtszustand für kaum noch vertretbar und befürchte, daß eine Berufung auf den sogenannten Übergangsbonus des Bundesverfassungsgerichts nicht mehr länger möglich sein wird. Seit Jahren weise ich auf die längst überfällige Lücke des Persönlichkeitsschutzes im Strafverfahren in so wichtigen Bereichen wie der Öffentlichkeitsfahndung, der Aktenauskunft und Akteneinsicht hin. Hierbei geht es nicht nur um Daten von „Gangstern“, sondern ebenso um Daten von Verbrechensopfern, Tatzeugen und Unbeteiligten – häufig ermittelt unter Zeugniszwang und unter Eingriff in die Privatsphäre. Daneben werden derzeit in allen Bereichen der Justiz im Zuge von Modernisierungsvorhaben umfassende Systeme der automatisierten Datenverarbeitung eingeführt mit der Folge, daß besonders schutzwürdige personenbezogene Daten auch hier in viel stärkerem Maße verfügbar werden als bisher.

Auch in der vergangenen 13. Legislaturperiode konnte der Entwurf eines Strafverfahrensänderungsgesetzes nicht abschließend beraten werden. Der in letzter Minute zustande gekommene Vorschlag scheiterte schließlich am Einspruch einer Landesregierung.

Ich halte es für dringend notwendig, wegen der mit der Datenerhebung, Verarbeitung und Nutzung verbundenen Rechtseingriffe in dieser Legislaturperiode unverzüglich bereichsspezifische Regelungen zu schaffen. Weitere Verzögerungen halte ich für nicht hinnehmbar. Im Hinblick auf die weniger datenschutzfreundlichen Vorstellungen im Bundesrat kann allenfalls mit einem Kompromiß gerechnet werden, den ich aber im Falle seiner Vertretbarkeit gegenüber der jetzigen unklaren Rechtssituation vorziehen würde (s. Nr. 6.2).

1.9 Entwicklung der Datenabgleiche: Wird der Bürger zum bloßen Objekt der Datensysteme?

Im Zuge der fortschreitenden Datenverarbeitung in den Verwaltungen hat sich der Ruf nach Datenabgleichen weiter verstärkt. Insbesondere im Bereich der Sozialleistungen wird der Datenabgleich quasi als Allheilmittel im Kampf gegen Leistungsmißbrauch angesehen. Jüngstes Beispiel ist der Entwurf des Steuerentlastungsgesetzes, nach dem künftig Mitteilungen des Bundesamtes für Finanzen über die Höhe der Zinseinnahmen und entsprechende Datenabgleiche zugunsten jedes Sozialleistungsträgers durchgeführt werden können, soweit dort Einkommen oder Vermögen durch den Versicherten zu offenbaren sind. Ursprünglich war diese Vorschrift, beschränkt auf die Anzahl der Freistellungsanträge, lediglich für Steuerverfahren geschaffen worden, bis schließlich der Abgleich mit der Arbeitsverwaltung eingeführt wurde (s. Nr. 20.2).

Die Zunahme dieser Datenabgleiche sehe ich mit Sorge, auch wenn es sein mag, daß jede Abgleichsregelung – für sich betrachtet – erfolgversprechend und unterstützenswert ist. Sozialdatenabgleiche sind letztlich flächendeckende Jedermann-Kontrollen. Nach dem Menschenbild des Grundgesetzes darf aber der Staat nicht jeder-

mann als potentiellen Rechtsbrecher – d. h. als solchen, der Leistungen mißbraucht – betrachten. Der Staat hat vielmehr davon auszugehen, daß die Bürger sich an Recht und Gesetz halten. Diese Redlichkeitsvermutung ist konstituierendes Merkmal unserer Verfassung.

In seinem Beschluß zu meinem 14. Tätigkeitsbericht hat der Deutsche Bundestag die Bundesregierung aufgefordert, vor der Einrichtung von Datenabgleichsverfahren jeweils zu prüfen, ob sie im Interesse des Gemeinwohls zur Erreichung eines konkreten Zieles erforderlich und verhältnismäßig sind. Auch seinerzeit war bereits die gewachsene Tendenz zur Einführung der Abgleichsverfahren festgestellt worden. Inzwischen hat diese Entwicklung ein Ausmaß angenommen, daß ich an den Bundesgesetzgeber appelliere, künftigen Forderungen nach Datenabgleichsverfahren mit Skepsis und Vorsicht zu begegnen. Angesichts der akuten Zunahme von Datenabgleichsverfahren ist zu befürchten, daß der Beitragszahler oder Leistungsbezieher damit zum bloßen Objekt der Datensysteme wird. Mit der Fehlerhäufigkeit beim Sozialhilfedatenabgleich habe ich mich in diesem Tätigkeitsbericht ausführlich auseinandergesetzt (s. Nr. 19.3) und davor gewarnt, den Empfänger einer Sozialleistung im „Trefferfall“ bereits des Mißbrauchs zu verdächtigen. Ohne weitere Recherche könnte dies zu Unrecht geschehen.

So hatte in der 13. Legislaturperiode das BMA das Ziel verfolgt, für alle Sozialleistungsbereiche eine zentrale, generalklauselartige Datenabgleichsvorschrift zu schaffen. Der diskutierte Entwurf wäre allerdings weit über das Ziel hinausgeschossen. Die Vorschrift sah weder Protokollierungen der Abgleiche noch andere Ansätze für eine angemessene Datenschutzkontrolle vor und berücksichtigte auch nicht, daß Datenabgleiche für Bürger transparent bleiben müssen. Damit Datenabgleiche nicht hinter dem Rücken der Betroffenen ablaufen, kommt der Transparenz bei Datenabgleichverfahren aus Datenschutzsicht entscheidende Bedeutung zu. Für mich ist unverzichtbar, daß die Bürger – wenigstens in allgemeiner Form – über die Abgleichsverfahren unterrichtet werden und zu Feststellungen aus dem Abgleich gehört werden.

An die Einführung neuer Datenabgleichsverfahren müssen daher strengere Voraussetzungen als bisher geknüpft werden. Insbesondere muß dargelegt werden, daß der beabsichtigte neue Datenabgleich zur Zielerreichung unabdingbar erforderlich ist. An den Deutschen Bundestag appelliere ich außerdem, die bestehenden Datenabgleichsverfahren in ihrer praktischen Bedeutung und Auswirkung auf den Verhältnismäßigkeits- und Erforderlichkeitsgrundsatz überprüfen zu lassen.

1.10 Beratungen und Kontrollen, insbesondere Beanstandungen

Die Kenntnis der tatsächlichen Abläufe bei der Erfüllung von Aufgaben ist Grundlage für die Beratung des Deutschen Bundestages und der Bundesregierung. Diese Kenntnis erlange ich überwiegend durch Kontrollen und Informationsbesuche. Deshalb sind die mir gesetzlich zugewiesenen Aufgaben der Beratung und Kontrolle von öffentlichen Stellen des Bundes, von Telekommunikationsunternehmen, von Unternehmen, die Postdienstleistungen erbringen, und von privaten Unternehmen, die unter das SÜG fallen, ausgesprochen wichtig. Im Berichtszeitraum habe ich zu zahlreichen Gesetzesvorhaben und datenschutzrechtlichen Fragen Bundesbehörden und sonstige öffentliche Stellen des Bundes sowie die genannten Unternehmen beraten und kontrolliert (s. hierzu **Anlage 2**).

Nach dem Bundesdatenschutzgesetz in Verbindung mit spezialgesetzlichen Regelungen, wie dem TKG oder PostG, muß ich Verstöße gegen datenschutzrechtliche Vorschriften förmlich beanstanden (§ 25 BDSG). Von einer Beanstandung kann ich u. a. absehen, wenn die Verstöße oder Mängel von geringer Bedeutung sind, aber auch wenn ein aus meiner Sicht datenschutzrechtliches Fehlverhalten sofort geändert wird. Leider ist die Zahl der Beanstandungen im Berichtszeitraum deutlich gestiegen. Zu den Beanstandungen im einzelnen siehe **Anlage 3**.

1.11 Hinweis für die Ausschüsse des Deutschen Bundestages

In der **Anlage 1** habe ich dargestellt, welche Kapitel dieses Berichts für welchen Ausschuß des Deutschen Bundestages von besonderem Interesse sein könnten.

2 Die notwendige Erneuerung des Datenschutzes

2.1 Die Umsetzung der europäischen Datenschutzrichtlinie

2.1.1 Die Richtlinie 95/46/EG vom 24. Oktober 1995

2.1.1.1 Versäumte Umsetzungsfrist – Verfehltes Umsetzungsziel

Die europäische Datenschutzrichtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, deren Entstehung und inhaltliche Konzeption ich in meinem 15. (Nrn. 33.1.1 bis 33.1.5) und 16. TB (Nrn. 2.1.1 bis 2.1.4) dargestellt habe, verpflichtet die Mitgliedstaaten, ihr Datenschutzrecht binnen dreier Jahre zu harmonisieren (Artikel 32 Abs. 1). Ausgehend von ihrer Unterzeichnung durch die Präsidenten von Europäischem Parlament und Ministerrat am 24. Oktober 1995 hätte die Richtlinie damit spätestens zum 24. Oktober 1998 in deutsches Recht umgesetzt sein müssen.

Indessen ist die dreijährige Umsetzungsfrist abgelaufen, ohne daß die deutsche Gesetzgebung ihrer Verpflichtung zur Anpassung des Datenschutzrechts an die in Brüssel beschlossenen Vorgaben nachgekommen wäre. Damit versäumte Deutschland, dessen Präsidentschaft im Europäischen Rat während der zweiten Hälfte des Jahres 1994 wesentlich zum Zustandekommen und der endgültigen Verabschiedung der Richtlinie beigetragen hat, die Frist und stand am Vorabend einer erneuten deutschen

Ratspräsidentschaft zu Beginn des Jahres 1999 mit leeren Händen da. Deutschland sah sich außerstande, der Europäischen Kommission zum Stichtag die fälligen Umsetzungsmaßnahmen zu notifizieren, d. h. eine Reform des BDSG, eine Anpassung der bereichsspezifischen Gesetze und novellierte Landesdatenschutzgesetze vorzulegen.

Daran ändert auch nichts, daß zur Zeit erst sechs Mitgliedstaaten die notwendigen gesetzgeberischen Schritte zur Umsetzung der Richtlinie gegangen sind, nämlich Italien, Griechenland, Finnland, Schweden, Portugal und das Vereinigte Königreich, wo das entsprechende Gesetz zwar verabschiedet ist, jedoch erst mit zeitlicher Verzögerung in Kraft treten wird. Aber auch in den meisten anderen Ländern ist der Umsetzungsprozeß schon relativ weit gediehen (s. u. Nr. 2.1.3). Leider zählt Deutschland – neben drei weiteren Mitgliedstaaten – zu den Schlußlichtern, über die es in einem kürzlich von der Kommission erstellten Tableau zum Sachstand der Umsetzungen in den Mitgliedstaaten lapidar heißt: „Parliamentary work yet to start".

Zu meinem Bedauern sollte die Frage der fristgerechten Umsetzung der Richtlinie im Berichtszeitraum denn auch in das Zentrum der Reformdiskussion rücken und die materiellen Probleme beinahe überlagern.

Bereits ein Jahr vor Ablauf der Umsetzungsfrist hatte ich gemeinsam mit meinen Kollegen aus den Ländern an die Bundesregierung appelliert, für eine fristgerechte Umsetzung der Richtlinie Sorge zu tragen. In der Entschließung „Novellierung des Bundesdatenschutzgesetzes und Modernisierung des Datenschutzrechts" der 54. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 23./24. Oktober 1997 (s. **Anlage 9**) wurde auf das Risiko eines Vertragsverletzungsverfahrens vor dem Europäischen Gerichtshof (EuGH) hingewiesen, dem der Mitgliedstaat Deutschland nach den Artikeln 169 und 170 des EG-Vertrages bei einer Klage durch die Europäische Kommission oder anderer Mitgliedstaaten im Falle nicht rechtzeitiger oder nicht ordnungsgemäßer Richtlinienumsetzung ausgesetzt ist.

Das federführende BMI versandte zwar im Dezember 1997 einen – innerhalb der Bundesregierung nicht vollständig abgestimmten – Referentenentwurf eines Gesetzes zur Änderung des Bundesdatenschutzgesetzes und anderer Gesetze an Ressorts, Landesregierungen, Fachverbände und an mich, wozu ich im Januar 1998 Stellung genommen habe (s. u. Nr. 2.1.2.1). Doch blieb das weitere Verfahren der Gesetzgebung im Laufe des Jahres 1998 im Stadium von weiteren Gesprächen und ministeriellen Entwürfen stecken. Nachdem im April 1998 über einen Kabinettsentwurf keine Einigung zustande kam, hat die alte Bundesregierung das Projekt zwar weiterverfolgt, aber zu keinem Ergebnis gebracht. Die neue Bundesregierung hat die Beratungen aufgenommen, die bis zum Redaktionsschluß dieses Tätigkeitsberichts jedoch noch nicht zu einem Kabinettsentwurf gediehen waren.

Diese Entwicklung ist für den Datenschutz, aber auch für die datenverarbeitenden Stellen, in Deutschland höchst nachteilig. Denn eine nicht fristgerechte Umsetzung führt zu Komplikationen bei der Teilnahme am harmonisierten „freien" Datenverkehr innerhalb des Europäischen Binnenmarktes. Aus innerstaatlicher Sicht liegen weitere Nachteile auf der Hand, da sich einerseits Verbesserungen des Datenschutzes für die Bürger, z. B. durch genauere Informationen über die Verarbeitung ihrer Daten, verzögern und andererseits eine zunehmende Zersplitterung des deutschen Datenschutzrechts droht. Denn den Ländern fehlt eine gemeinsame Orientierung für die Anpassung ihrer Landesdatenschutzgesetze. Hessen und Brandenburg haben mit ihren novellierten Datenschutzgesetzen schon nicht mehr auf den Bund gewartet.

Ich appelliere daher an die neue Bundesregierung, für eine rasche Umsetzung der Richtlinie Sorge zu tragen.

2.1.1.2 Direktwirkung der Richtlinie durch unmittelbare Anwendung nach Ablauf der Umsetzungsfrist

Da die notwendig gewordenen Anpassungen der Vorschriften des BDSG und anderer bereichsspezifischer Bundesgesetze an die Vorgaben der Richtlinie nicht rechtzeitig erfolgt sind, stellt sich die Frage nach der Vorgehensweise datenverarbeitender Stellen des Bundes seit Ablauf dieses Termins am 24. Oktober 1998.

Nach ständiger Rechtsprechung des EuGH finden Regelungen einer Richtlinie nach Ablauf der Umsetzungsfrist auch ohne Umsetzung in nationales Recht zugunsten der Bürger in ihrem Verhältnis gegenüber dem Staat – nicht jedoch im Verhältnis der Bürger untereinander – unmittelbare Anwendung. Voraussetzung für eine solche Direktwirkung ist, daß der einzelne sich auf ein in einer Richtlinie ihm gegenüber hinreichend bestimmtes und unbedingt eingeräumtes Recht berufen kann, die Vorschrift mithin „self-executing" ist. Hierbei ist ferner zu beachten, daß der EuGH seit 1991 auf eine Schadensersatzpflicht der Mitgliedstaaten bei fehlender Befolgung von Gemeinschaftsrecht im Falle der Nichtumsetzung einer Richtlinie erkennt. Danach kann der einzelne, wenn ihm eine Richtlinie ein inhaltlich bestimmbares Recht einräumt, das infolge fehlender Umsetzung nicht effektiv wurde, einen nach Ablauf der Umsetzungsfrist daraus kausal entstandenen Schaden – gegenüber dem Mitgliedstaat – geltend machen.

Die Voraussetzungen direkter Wirkung liegen bei einer Reihe von Regelungen der Datenschutzrichtlinie vor. Um die damit im Zusammenhang stehenden komplizierten Fragen nicht erst aus Anlaß zu erwartender Nachfragen zu erörtern und einer Beantwortung zuzuführen, erschien es mir empfehlenswert, die Bundesministerien hierauf aufmerksam zu machen (s. **Anlage 19**).

In diesem Zusammenhang ist insbesondere an die Vorgaben der Richtlinie in den Artikeln 2, 3 und 9 betreffend die Begriffsbestimmungen, den Anwendungsbereich und die Verarbeitung personenbezogener Daten im Hinblick auf die Meinungsfreiheit zu denken. So geht die Richtlinie von einem umfassenden Verarbeitungs- und Dateibegriff aus. Die Rechte des einzelnen gelten dementsprechend für einen erweiterten Anwendungsbereich.

Außerdem ist an die Informations- und Widerspruchsrechte nach den Artikeln 10, 11 und 14 zu erinnern. Schon jetzt haben die datenverarbeitenden Stellen ein Vorbringen von Betroffenen, das als Widerspruch zu werten ist, auf seine Begründetheit zu prüfen und entsprechend zu berücksichtigen, wie es in Artikel 14 vorgesehen ist. Und nach den Artikeln 10 und 11 enthält der Betroffene schon jetzt, wenn die Situation es nach Treu und Glauben erfordert, „weitere Informationen“, soweit sie ihm noch nicht vorliegen, die sich beispielsweise auf folgendes beziehen können:

– die Empfänger oder Kategorien der Empfänger der Daten,
– das Bestehen von Auskunfts- und Berichtigungsrechten bezüglich ihn betreffender Daten,
– die Frage, ob die Beantwortung der Fragen obligatorisch oder freiwillig ist, sowie mögliche Folgen einer unterlassenen Beantwortung (Artikel 10) und
– die Datenkategorien, die verarbeitet werden (Artikel 11).

Weiterhin darf eine Auskunft an den Betroffenen nur unter den in der Richtlinie bestimmten Voraussetzungen (Artikel 13) verweigert werden; nur in diesem Rahmen sind die entsprechenden Regelungen der §§ 19 Abs. 4 und 34 Abs. 4 BDSG anwendbar.

Schließlich ist das grundsätzliche Verarbeitungsverbot sog. sensitiver Daten zu beachten mit der Folge, daß die Erlaubnistatbestände des BDSG teilweise keine Anwendung mehr finden. So dürfen Gesundheitsdaten etwa außerhalb des Anwendungsbereiches des angemessene Garantien bietenden Sozialversicherungsrechts und außer durch ärztliches Personal ohne Einwilligung des Betroffenen nicht mehr verarbeitet werden. Dem ist beispielsweise im Rahmen des Dienst- und Arbeitsrechts Rechnung zu tragen.

2.1.2 Die Novellierung des Bundesdatenschutzgesetzes – Forderungen an den Reformgesetzgeber

2.1.2.1 Ein erster Arbeitsentwurf aus dem BMI in der abgelaufenen Legislaturperiode

Im Frühsommer 1997 kursierte ein erster Arbeitsentwurf aus dem Fachreferat des federführenden BMI, der im darauffolgenden Dezember auch mir zur Prüfung und Begutachtung vorgelegt wurde (s. o. Nr. 2.1.1.1).

In meiner Stellungnahme vom 30. Januar 1998 habe ich deutlich gemacht, daß die Forderungen der Datenschutzbeauftragten nach einer umfassenden Novellierung des BDSG, wie sie zuletzt in der Entschließung „Novellierung des Bundesdatenschutzgesetzes und Modernisierung des Datenschutzrechts“ der 54. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 23./24. Oktober 1997 (s. **Anlage 9**) und in meinem 16. Tätigkeitsbericht (Nr. 2.1.5) dargelegt worden sind, in dem Entwurf nicht berücksichtigt werden. Ich habe klargestellt, daß eine Anpassung an die heutige Informationstechnologie und an die Verhältnisse der modernen Informationsgesellschaft unverändert dringlich ist. In diesem Zusammenhang verweise ich auch auf die Entschließung des Deutschen Bundestages zu meinem 16. Tätigkeitsbericht (s. **Anlage 4**)

Bei der Formulierung des Entwurfes ist lediglich versucht worden, die Bestimmungen der Richtlinie durch punktuelle – und dadurch äußerst zahlreiche – Einfügungen und Änderungen dem bestehenden Regelungswerk aufzupfropfen. Das Ergebnis wäre ein noch schwerer lesbares Gesetzeswerk geworden, als dies bereits für das geltende BDSG zutrifft. Ein solches Vorgehen birgt nicht nur die Gefahr in sich, daß die Bürger der Grundidee des Datenschutzes entfremdet werden, sondern es bleiben die in anderen Bereichen bekannten Schwierigkeiten für Rechtsanwender und Betroffene, ein klares Bild zu gewinnen. Daß auch einfache Formulierungen möglich sind, zeigen die insoweit vorbildlichen Datenschutzvorschriften des Informations- und Kommunikationsdienstegesetzes (IuKDG) und des Mediendienste-Staatsvertrages (MDStV).

Beim Dateibegriff befürworte ich daher eine vollständige Übernahme der Definition aus der Richtlinie. Die – nur historisch erklärbare – Dreiteilung des Verarbeitungsbegriffs in „Erheben“, „Verarbeiten“ und „Nutzen“ sollte überwunden und der einheitliche Verarbeitungsbegriff der Datenschutzrichtlinie zugrunde gelegt werden. Die bei der Datenerhebung für eigene Zwecke neu eingefügte Zweckbindungsregel in § 28 Abs. 2 habe ich dagegen begrüßt. Andererseits schrieb Absatz 3 eine vielkritisierte Fehlleistung der alten Fassung fort, indem der Betroffene auch künftig nicht auf sein Widerspruchsrecht gegenüber der Nutzung oder Übermittlung seiner Daten für Zwecke der Werbung oder der Markt- oder Meinungsforschung zu unterrichten wäre. Ferner hätte ich mir zu Beginn des Gesetzes eine Bezugnahme auf den Schutz der Privatsphäre und das Recht auf informationelle Selbstbestimmung gewünscht, um den Grundrechtsbezug hervorzuheben. Auch die Regelung der technischen und organisatorischen Maßnahmen in Form einer „Anlage" entspricht nicht deren zentraler Bedeutung. Wünschenswert wären im übrigen Regelungen zur Netzkontrolle und zur Sicherstellung der Revisionsfähigkeit der DV-Systeme gewesen.

Verschiedene Defizite sah ich unter anderem auch bei der Regelung des Entwurfs zu § 29 (Geschäftsmäßige Datenerhebung und -speicherung zum Zwecke der Übermittlung), § 33 (Benachrichtigung des Betroffenen) und § 34 (Auskunft an den Betroffenen). Bei § 29 habe ich die fehlende Hinweispflicht auf die Möglichkeit des Widerspruchs kritisiert. § 33 setzt die Vorgaben von Artikel 11 der Richtlinie im Hinblick auf die Informationen für den Fall nicht vollständig um, daß die Daten nicht bei der betroffenen Person erhoben wurden. Schließlich erschienen mir die Einschränkungen des Auskunftsrechts des Betroffenen in § 34, gemessen an den Vorgaben der Artikel 12 und 13 der Richtlinie, als zu weitgehend, weshalb ich für eine Streichung plädiert habe.

Neben diesen Einzelheiten, die die Mängel dieses ersten Umsetzungsversuches erkennen lassen, fehlte es in dem Entwurf aber auch an Ansätzen, die mittlerweile vor-

dringlich gewordenen neuen Problemfelder des Datenschutzes im nicht-öffentlichen Bereich mit gesetzgeberischen Mitteln anzugehen. Zu nennen sind hier insbesondere folgende Punkte, für die genaue gesetzliche Vorgaben dringend erforderlich sind:

– Videoaufzeichnungen im nicht-öffentlichen Bereich,
– Gesetzliche Regelung für die Verwendung von Chipkarten,
– Arbeitnehmerdatenschutz,
– Regelung der Medien entsprechend Artikel 9 der Richtlinie,
– Verschärfte Anforderungen an Auskunfteien, Adreßhändler und Direktmarketing,
– Widerspruch gegen Werbung und
– Regelung der Datenverarbeitung bei Detekteien und privaten Sicherheitsdiensten, wobei der Regelungsstandort hier die Gewerbeordnung wäre.

Bis zum Frühjahr des Jahres 1998 fanden mehrere Gespräche statt, die allerdings den Unterschied zwischen Minimalismus und Modernisierung, zwischen einem „Das Unvermeidliche tun“ und einem an den Entwicklungen der IuK-Technik orientierten Reformansatz nur noch deutlicher werden ließen. Da ursprünglich das BDSG noch in der abgelaufenen Legislaturperiode novelliert werden sollte, hatte ich zunächst Verständnis dafür gezeigt, daß angesichts des bestehenden Zeitdrucks und der Notwendigkeit, auch bereichsspezifische Regelungen in die Novelle einzubeziehen, in einem ersten Schritt nur eine eng an der Richtlinie orientierte Reform beabsichtigt war. Nachfolgend wurde die Novellierungsdiskussion dann kurzerhand von der Tagesordnung abgesetzt und auf die Zeit nach der Bundestagswahl im Herbst 1998 vertagt.

Angesichts der eindeutigen europäischen Vorgaben und der offenkundigen Dringlichkeit der anstehenden Novellierung des BDSG ist dieser schleppende Gang des Gesetzgebungsverfahrens bis zum Ende der vergangenen Legislaturperiode schwer verständlich. Aus meiner Sicht kann nur festgestellt werden, daß die alte Bundesregierung der Reform des Datenschutzrechts nicht die nötige Priorität eingeräumt hatte.

2.1.2.2 Erwartungen an den neuen Gesetzgeber

– Enquete-Kommission des Deutschen Bundestages zur Informationsgesellschaft

Daß der Wille zu einer Modernisierung des Datenschutzes in hohem Maße – auch und gerade im parlamentarischen Bereich – durchaus vorhanden ist, zeigen die Ergebnisse der vom Deutschen Bundestag eingesetzten Enquete-Kommission „Zukunft der Medien in Wirtschaft und Gesellschaft – Deutschlands Weg in die Informationsgesellschaft“ (BT-Drs. 13/11004). Diese betonte noch im Herbst des vergangenen Jahres in ihrem vierten Zwischenbericht und in ihrem Schlußbericht die Bedeutung des Datenschutzes und mahnte in diesem Zusammenhang an, daß die anstehende Umsetzung der EG-Datenschutzrichtlinie *„zu einer umfassenden Novellierung des Bundesdatenschutzgesetzes und anderer datenschutzrechtlicher Regelungswerke genutzt werden sollte“.*

Dieser Sichtweise des Parlaments kann ich nur zustimmen. Meine Erwartungen richten sich daher auf den neugewählten Bundestag, daß er die Persönlichkeitsrechte noch deutlicher herausstellt und dem Datenschutzrecht den Platz verschafft, der ihm in der Informationsgesellschaft zukommt.

– Der Entwurf für ein Eckwerte-Papier der SPD-Bundestagsfraktion

Ein kurz nach der Bundestagswahl bekanntgewordener Entwurf für ein Eckwerte-Papier der SPD-Bundestagsfraktion „Modernes Datenschutzrecht für die (globale) Wissens- und Informationsgesellschaft“ macht sich in begrüßenswerter Weise langjährige Forderungen an den Gesetzgeber aus Datenschutzsicht in zahlreichen Punkten zu eigen. So nimmt er ausdrücklich auf die Entschließung „Modernisierung und europäische Harmonisierung des Datenschutzrechts“ der 51. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 14./15. März 1996 (s. 16. TB Anlage 15) Bezug und stellt zu Recht fest, daß die aufgrund der Umsetzung der europäischen Datenschutzrichtlinie notwendige Erneuerung der datenschutzrechtlichen Rahmenbedingungen nicht nur als Beitrag zur europäischen Integration zu verstehen ist, sondern als Aufforderung und Chance, den Datenschutz fortzuentwickeln.

Das Papier geht auch auf meine Forderungen an den Gesetzgeber aus meinem 16. Tätigkeitsbericht (Nr. 2.1.5) ein und ist mit mir einer Meinung, daß die Entwicklung eines modernen Datenschutzkonzeptes Gegenstand zentraler Reform- und Modernisierungsüberlegungen der vor uns liegenden Jahre sein wird. Es teilt meine Erwartungen an eine neue Politik zum Schutz der Privatsphäre, meine Kritik an „minimalistischen“ Vorstellungen und meine Forderungen nach einem umfassenden Regelungsansatz, der auch absehbare künftige Entwicklungen berücksichtigt. Positiv hervorzuheben ist besonders, daß der Entwurf den Datenschutz als wesentliches Element der entstehenden Informationsgesellschaft begreift.

– Der Gesetzentwurf der Fraktion Bündnis 90/Die Grünen

Bereits am 11. November 1997 hatte die Fraktion Bündnis 90/Die Grünen einen Gesetzentwurf zur Novellierung des BDSG vorgelegt (BT-Drs. 13/9082). Der Entwurf, der sich auch auf die Entschließung „Modernisierung und europäische Harmonisierung des Datenschutzrechts“ der 51. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 14./15. März 1996 (s. 16. TB Anlage 15) beruft, macht sich deren Positionen in zahlreichen Punkten zu eigen und nimmt mehrfach auf meinen 16. Tätigkeitsbericht (Nr. 2.1.5) Bezug. Er schließt sich meiner Feststellung an, daß eine Reduzierung der Novellierung des BDSG auf die unumgänglichen Anpassungen an die europäischen Vorgaben eine baldige erneute Novellierung erforderlich machen

würde, was weder im Interesse der Rechtsanwender noch allgemein im Interesse der Rechtssicherheit liegen könne. Aus diesem Grund verfolgt er auch einen umfassenden Regelungsansatz, der absehbare künftige Entwicklungen berücksichtigt.

Der Entwurf strebt nicht nur eine vollständige Umsetzung der Vorgaben der Richtlinie an, sondern sieht auch Regelungen zu neuen Technologien wie Verbundverfahren, Chipkarten und Videoüberwachung vor. Darüber hinaus ist vorgesehen, das BDSG an die neuen Entwicklungen der Informationstechnik im Sinne der Forderungen der Datenschutzbeauftragten zu datenschutzfreundlichen Technologien (s. auch Nr. 8.5) anzupassen. Dem dienen eine Pflicht zur Verschlüsselung sensibler Daten, das Datenschutz-Audit sowie Regelungen zur Datensparsamkeit, Anonymisierung und Pseudonymisierung.

Der Entwurf war zur Beratung an den Innenausschuß verwiesen worden. Diese fand jedoch in der abgelaufenen Legislaturperiode nicht mehr statt, da die damaligen Koalitionsfraktionen sich auf eine gemeinsame Beratung mit einem eventuellen Regierungsentwurf festgelegt hatten.

– Die Beschlüsse des 62. Deutschen Juristentages

Auf der Linie des Entwurfs für ein Eckwerte-Papier der SPD-Bundestagsfraktion und des Gesetzentwurfs der Fraktion Bündnis 90/Die Grünen liegen auch die Beschlüsse des 62. Deutschen Juristentages vom September 1998 in Bremen (s. **Anlage 5**), der in seiner Abteilung Öffentliches Recht das Thema beriet: Geben moderne Technologien und die europäische Integration Anlaß, Notwendigkeit und Grenzen des Schutzes personenbezogener Informationen neu zu bestimmen? Dort wurde mit überwältigender Mehrheit beschlossen, daß technischer Selbstschutz und Selbstregulierungen, etwa in der Form eines Datenschutz-Audits, Eckpfeiler jeder Neuregelung sind und daß das künftige Informationsrecht sich wirkungsorientiert u. a. an den Leitlinien von Datenvermeidung und Datensparsamkeit, Anonymisierung und Pseudonymisierung personenbezogener Daten ausrichten soll.

– Fortsetzung der Reformarbeiten im BMI

Das BMI nahm inzwischen die Vorarbeiten zur Novellierung des BDSG wieder auf. Ausgangspunkt ist zwar der Entwurf vom April 1998. Zusätzlich sollen jedoch wichtige Elemente zur Modernisierung aufgenommen werden, was ich sehr begrüße. So werden insbesondere Regelungen zur Zulässigkeit von Videoaufzeichnungen, zum Einsatz von Chipkarten, zur Einrichtung eines Datenschutz-Audits sowie im Hinblick auf das Prinzip der Datenvermeidung und Datensparsamkeit erörtert. In den nächsten Verhandlungsschritten werde ich Wert darauf legen, daß – über diese Punkte hinaus – auch an den bisher erhobenen, weitergehenden Forderungen zu einer umfassenden Novellierung des Datenschutzrechts festgehalten wird, wie sie zuletzt noch einmal in der Entschließung „Dringlichkeit der Datenschutzmodernisierung“ der 56. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 5./6. Oktober 1998 (s. **Anlage 14**) zusammengefaßt worden sind. Wegen des hohen zeitlichen Drucks zur Umsetzung der Richtlinie kann es notwendig werden, die Reform in zwei Phasen zu verwirklichen. Sofern dabei die erwähnten Elemente der Modernisierung in die erste Phase aufgenommen werden und die Verwirklichung der zweiten Phase in der laufenden Legislaturperiode fest eingeplant wird, ist dagegen unter den gegebenen Umständen aus meiner Sicht nichts einzuwenden.

2.1.3 Die Umsetzung der Richtlinie in den einzelnen Mitgliedstaaten der Europäischen Union

Auch in einer Reihe anderer Mitgliedstaaten der Europäischen Union ging es mit der Umsetzung der Datenschutzrichtlinie nur schleppend voran. Zum Stichtag 24. Oktober 1998 konnten nur fünf Mitgliedstaaten die rechtzeitige Umsetzung nach Brüssel melden, nämlich Italien, Griechenland, Schweden, Portugal und Großbritannien, dessen Gesetz allerdings erst später voll in Kraft treten wird. Als sechster und siebenter Mitgliedstaat sind inzwischen Belgien und Finnland hinzugekommen (Stand: März 1999). Zwar sind in allen anderen Ländern der Gemeinschaft die entsprechenden Gremien mit der Anpassung des nationalen Datenschutzrechts befaßt, jedoch gab es in Deutschland (s. o. Nr. 2.1.1.1) sowie in Frankreich, Luxemburg und Österreich bislang noch keine parlamentarische Beratungen.

Der Stand der Umsetzung stellte sich in den einzelnen Mitgliedstaaten am 24. Oktober 1998 wie folgt dar:

Belgien: Der Gesetzentwurf zur Umsetzung der Richtlinie wurde nach Stellungnahme des Staatsrates vom Januar 1998 im April desselben Jahres erneut dem Parlament vorgelegt und wird derzeit im Rechtsausschuß beraten.

Dänemark: Der Gesetzentwurf zur Umsetzung lag dem Parlament im April 1998 vor und wurde im Oktober desselben Jahres in erster Lesung behandelt.

Finnland: Nachdem ein parlamentarischer Ad-hoc-Ausschuß zur Umsetzung der Richtlinie seine Arbeit im Jahre 1997 beendet hatte, konnte der Gesetzentwurf im darauffolgenden Jahr dem Parlament unterbreitet werden, das ihn im Herbst 1998 verabschiedete.

Frankreich: Die parlamentarischen Arbeiten haben noch nicht begonnen. Auch ein Regierungsentwurf steht noch aus.

Griechenland: Das griechische Parlament verabschiedete im März 1997 das Umsetzungsgesetz, das am 10. April 1997 verkündet wurde. Mit dem Gesetz, das den Vorgaben der Richtlinie in enger Anpassung folgt, setzte Griechenland, das bis dato noch über kein Datenschutzgesetz verfügte, die Richtlinie als erster Mitgliedstaat der Europäischen Union in nationales Recht um.

Großbritannien: Der dem Parlament im Januar 1998 unterbreitete Gesetzentwurf wurde Anfang Juli 1998 verabschiedet. Die Königliche Zustimmung (Royal Assent) erfolgte am 16. Juli 1998. Zum eigentlichen Inkrafttreten des Data Protection Act 1998 sind weitere

gesetzgeberische Schritte auf dem Verordnungswege (Secondary Legislation) notwendig.

Irland: In Irland liegt ein Regierungsentwurf vor, der bislang jedoch noch nicht parlamentarisch beraten wurde.

Italien: In Italien, das neben Griechenland zum Zeitpunkt der Verabschiedung der Richtlinie im Oktober 1995 noch kein Datenschutzgesetz besaß, verabschiedete das Parlament im Dezember 1996 den Regierungsentwurf eines Datenschutzgesetzes vom Juni desselben Jahres. Am 8. Mai 1997 trat das italienische Datenschutzgesetz in Kraft. Bereits mit Wirkung vom übernächsten Tag wurde das Gesetz per Dekret vom 9. Mai 1997 in zahlreichen wichtigen Punkten, insbesondere aufgrund gesetzessystematischer Unstimmigkeiten der gerade in Kraft getretenen Vorschriften, wieder geändert.

Luxemburg: Nachdem ein Gesetzentwurf aus dem Jahre 1997 zurückgezogen worden war, bereitet das Justizministerium derzeit einen erneuten Entwurf vor.

Niederlande: Ein Regierungsentwurf von Februar 1998 wurde im zuständigen Parlamentsausschuß beraten. Nach dessen Stellungnahme vom Juni 1998 steht die Plenarbehandlung durch das Parlament noch aus.

Österreich: Der Gesetzentwurf des federführenden Bundeskanzleramtes wurde dem Datenschutzrat zur Stellungnahme zugeleitet. Eine überarbeitete Entwurfsfassung ist dem Parlament noch zuzuleiten.

Portugal: Ein Gesetzentwurf vom April 1998 konnte nach Änderung der portugiesischen Verfassung – diese enthielt Datenschutzregelungen, die in Teilen restriktiver waren als die Richtlinie – vom Parlament am 25. September 1998 verabschiedet werden.

Schweden: Eine teilweise Umsetzung der Richtlinie erfolgte durch das Gesetz vom 16. April 1998. Weitere Regelungen zur Umsetzung der Richtlinie erfolgten durch Rechtsverordnungen, die im September 1998 verabschiedet wurden und im darauffolgenden Oktober in Kraft getreten sind.

Spanien: Ein Regierungsentwurf vom Juli 1998 befindet sich noch in parlamentarischer Beratung.

2.2 Die Brüsseler Datenschutzgruppe nach Artikel 29 der EG-Richtlinie

2.2.1 Arbeitsschwerpunkte und Ergebnisse

Über Aufgaben und Zusammensetzung der Datenschutzgruppe sowie ihre vorläufige Geschäftsordnung habe ich im 16. TB (Nr. 2.1.3) berichtet. Seit ihrer konstituierenden Sitzung am 17. Januar 1996 haben sich die Mitglieder der Gruppe bis zum Frühjahr 1999 in kürzer werdenden Intervallen fünfzehnmal in Brüssel getroffen und verschiedene Aspekte des europäischen Datenschutzes diskutiert. Der Bogen der bisher behandelten Themen spannt sich vom Stand der Umsetzung der Richtlinie in den Mitgliedstaaten über Medien- und Internetfragen bis hin zu den Aktivitäten anderer Organisationen wie der OECD und des Europarates. Dabei befaßt sich die Datenschutzgruppe nicht nur mit Anfragen der Kommission, sondern – wie in Artikel 30 Abs. 3 der Richtlinie vorgesehen – auch mit datenschutzrechtlichen Punkten von gemeinschaftsweiter Relevanz. Mittlerweile nehmen die Datenschutzbeauftragten von Norwegen und Island an den Gruppensitzungen teil.

Der Öffentlichkeit hat die Gruppe bisher Teile ihrer Beratungsergebnisse in 17 Papieren (Working Papers – WP) zugänglich gemacht (Zusammenstellung der von der Arbeitsgruppe angenommenen Dokumente s. **Anlage 18**). Bei diesen Papieren handelt es sich u. a. um die ersten beiden Jahresberichte der Gruppe (WP 3 und WP 14) und fünf Ausarbeitungen zu einer der Kernfragen des gemeinschaftlichen Datenschutzrechts, nämlich der Übermittlung personenbezogener Daten in Drittländer.

2.2.2 Datenübermittlungen in Drittstaaten – Die transatlantische Debatte

Seit ihrer ersten Sitzung befaßt sich die Artikel 29-Gruppe eingehend mit dieser Problematik. Im Vordergrund stehen die Fälle, in denen in einem Drittstaat ein angemessener Schutz i.S.d. Artikel 25 der Richtlinie nicht sichergestellt ist und – sofern keine der einschlägigen Ausnahmebestimmungen nach Artikel 26 anwendbar ist – die Datenübermittlungen äußerstenfalls blokkiert werden müßten. Da somit in letzter Konsequenz Verbote von Datentransfers durch die Kontrollstellen der Mitgliedstaaten drohen, ist die Reaktion in den hauptsächlich betroffenen Staaten – und insbesondere in den USA – entsprechend heftig.

Dabei wird die transatlantische Debatte von kontroversen Ausgangspunkten geführt. Essentialia für eine hinreichende Adäquanz bilden nach europäischen Vorstellungen eine klare Zweckbindung, ein funktionierendes Beschwerdesystem und eine effiziente Kontrollinstanz, deren rechtliche Verankerung vorzugsweise durch Gesetz erfolgen sollte. Dagegen lehnt die amerikanische Seite gesetzliche Regelungen, jedenfalls in der uns bekannten herkömmlichen Form allgemeiner Datenschutzgesetze, ab. Dies sei dem common law systemfremd. Es sei aber auch überflüssig, da richtiger Datenschutz ebensogut durch die Selbstregulierung der betroffenen Wirtschaftskreise sichergestellt werden könne. Die Effizienz des self-regulation-Systems wird wiederum in Europa bezweifelt und die behauptete Systemwidrigkeit gesetzlicher Regelungen – unter anderem durch den Hinweis auf die zahlreichen bereichsspezifischen Gesetze wie etwa den Fair Credit Reporting Act oder den Video Privacy Protection Act – bestritten. Und insbesondere wird der kanadische Nachbar zum Gegenbeweis herangezogen, der trotz seiner Angehörigkeit zur Rechtsfamilie des common law nicht nur Datenschutzgesetze für den öffentlichen Bereich in Bund und Ländern kennt, sondern darüber hinaus seine Bereitschaft angekündigt hat, dieses Gesetzesrecht auf die private Wirtschaft im ganzen auszudehnen (s. u. Nr. 32.3).

Mit dem Ziel eines konstruktiven Dialogs hat die Datenschutzgruppe in den vergangenen Jahren gemeinsame

Positionen erarbeitet und in Arbeitspapieren niedergelegt:

– Erste Leitlinien für die Übermittlung personenbezogener Daten in Drittländer – Mögliche Ansätze für eine Bewertung der Angemessenheit (WP 4),

– Beurteilung der Selbstkontrolle der Wirtschaft: Wann ist sie ein sinnvoller Beitrag zum Niveau des Datenschutzes in einem Drittland? (WP 7),

– Erste Überlegungen zur Verwendung vertraglicher Bestimmungen im Rahmen der Übermittlungen personenbezogener Daten an Drittländer (WP 9) und

– Übermittlungen personenbezogener Daten an Drittländer: Anwendung von Artikel 25 und 26 der Datenschutzrichtlinie der EU (WP 12).

Das Dokument WP 12 verabschiedete die Gruppe am 24. Juli 1998 zum vorläufigen Abschluß als Synthesepapier, das die vorgenannten Dokumente zusammenfaßt und eine Reihe umfassender und in sich schlüssiger Vorschläge für die Anwendung der Artikel 25 und 26 der Richtlinie bietet.

In Artikel 25 Abs. 1 ist der Grundsatz aufgeführt, daß die Mitgliedstaaten die Übermittlung in ein Drittland nur gestatten, wenn dieses Land ein angemessenes Schutzniveau gewährleistet, wobei in Absatz 2 darauf verwiesen wird, daß *„die Angemessenheit ... unter Berücksichtigung aller Umstände beurteilt“* wird. Zur Sicherung einer einheitlichen Praxis ist nach Absatz 6 der Kommission die Befugnis übertragen, festzustellen, daß ein Drittland aufgrund seiner innerstaatlichen Rechtsvorschriften oder internationaler Verpflichtungen ein angemessenes Schutzniveau i.S.d. Absatzes 2 gewährleistet. Diese internationalen Verpflichtungen können sich wiederum vor allem aus Verhandlungen mit der Kommission (nach Absatz 5) ergeben.

So widmet sich das Synthesepapier denn auch zunächst der zentralen Frage des angemessenen Schutzniveaus. Es erklärt eingangs, was unter „angemessen“ zu verstehen ist und stellt danach einen Rahmen für die Frage auf, wie die Angemessenheit des Schutzes im konkreten Fall beurteilt werden kann. Unter inhaltlichen Gesichtspunkten sind dabei die folgenden Grundsätze unbedingt zu berücksichtigen:

– Der Grundsatz der Beschränkung der Zweckbestimmung,

– der Grundsatz der Datenqualität und -verhältnismäßigkeit,

– der Grundsatz der Transparenz,

– der Grundsatz der Sicherheit,

– das individuelle Recht auf Auskunft, Berichtigung und Widerspruch sowie

– der Grundsatz der Beschränkung der Weiterübermittlung in andere Drittländer.

Für spezifische Arten der Verarbeitung – wie bei sensitiven Daten, beim Direktmarketing und bei automatisierter Einzelentscheidung – gelten besondere Grundsätze.

Eine unabhängige Kontrollbehörde nach europäischem Vorbild kann naturgemäß nicht gefordert werden, wohl aber (andere) verfahrensmäßige Vorkehrungen oder Durchsetzungsmechanismen, die vergleichbares leisten. Das Synthesepapier fordert daher entsprechende Strukturen, die die folgenden Ziele sichern:

– Gewährleistung einer guten Befolgungsrate der Vorschriften,

– Unterstützung und Hilfe für einzelne betroffene Personen bei der Wahrnehmung ihrer Rechte,

– Gewährleistung angemessener Entschädigung für die geschädigte Partei bei Verstoß gegen die Bestimmungen.

Im weiteren beschäftigt sich das Dokument mit Übermittlungen in Länder, die das Übereinkommen 108 des Europarates aus dem Jahre 1981 ratifiziert haben und behandelt danach Fragen im Zusammenhang mit Übermittlungen, bei denen der Schutz personenbezogener Daten beim Empfänger hauptsächlich oder vollständig über Mechanismen der freiwilligen Selbstkontrolle und nicht auf gesetzlichem Wege erfolgt. Die Instrumente der Selbstkontrolle haben sich an den erwähnten inhaltlichen Grundsätzen und verfahrensrechtlichen Durchsetzungsmechanismen zu orientieren.

Bei der Bewertung des Schutzniveaus in einem Drittstaat kommt somit der Grundgedanke zum Tragen, daß einem in seinem Wesensgehalt unabdingbaren Bestand materieller Kriterien mittels variabler Verfahrensformen Durchsetzung verschafft wird. Diese Vorgehensweise wird im Anhang des Dokuments einer ersten Prüfung unterzogen, indem anhand mehrerer anschaulicher Fallstudien gezeigt wird, wie der zuvor beschriebene Ansatz in der Praxis durchgesetzt werden könnte.

2.2.3 Das Ausschußverfahren nach Artikel 31 der EG-Richtlinie

Zusätzlich zu der Datenschutzgruppe nach Artikel 29 sieht die Richtlinie in Artikel 31 die Bildung eines Verwaltungsausschusses mit Regierungsvertretern vor. Während ersteres Gremium die Kommission mit Praxiserfahrung aus unabhängiger Datenschutzsicht versorgen soll, dient das Ausschußverfahren dazu, die regierungsamtliche Mitwirkung der Mitgliedstaaten zu gewährleisten und dabei die Kommission bei der Ausübung der ihr übertragenen Entscheidungsbefugnisse zu unterstützen. Der Ausschuß, der seine Beratungen im vergangenen Jahr aufnahm, befaßte sich ebenfalls mit dem Thema des Drittstaatentransfers, wobei er sich auch auf Vorarbeiten der Artikel 29-Gruppe stützen konnte.

2.3 Neue Datenschutzregelungen für die Organe der EU in den europäischen Verträgen

Die europäischen Institutionen, und hier vor allem die Kommission, verarbeiten im Rahmen ihrer Tätigkeiten ständig große Mengen personenbezogener Daten. So tauscht die Kommission personenbezogene Daten mit den Mitgliedstaaten im Rahmen der Gemeinsamen

Agrarpolitik, bei der Verwaltung des Zollsystems oder der Strukturfonds aus und ist Empfänger millionenfach übermittelter Daten auf den Gebieten etwa des Subventionswesens oder des Wettbewerbsrechts (Fusionskontrolle). Da aber die Richtlinie nach Artikel 34 ausschließlich an die Mitgliedstaaten gerichtet ist, erstreckt sich ihr Geltungsbereich nicht auf die Organe und Einrichtungen von Europäischer Gemeinschaft und Union.

Diese Lücke im europäischen Datenschutzgefüge habe ich aus Datenschutzsicht seit langem bemängelt (vgl. 12. TB S. 49, 13. TB S. 57 f., 15. TB Nr. 33.6 und 16. TB Nr. 2.2). Mit Blick auf die 1996 begonnene und im Herbst 1997 abgeschlossene Regierungskonferenz zur Überprüfung des Vertrages über die Europäische Union von Maastricht hatten die europäischen Datenschutzbeauftragten eine von mir vorgelegte Erklärung verabschiedet, die als „Kopenhagener Resolution“ (s. 16. TB Anlage 4) Forderungen nach Verankerung eines europäischen Grundrechts auf Datenschutz im Grundrechtskatalog einer geschriebenen EU-Verfassung enthielt sowie Maßnahmen zur Schaffung eines verbindlichen Datenschutzrechts für die Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen von Gemeinschaft und Union und zur Einrichtung eines unabhängigen europäischen Datenschutzbeauftragten empfahl. Im gleichen Sinne hatte sich die 50. Konferenz der Datenschutzbeauftragten des Bundes und der Länder in ihrer Entschließung vom 9./10. November 1995 zur „Weiterentwicklung des Datenschutzes in der Europäischen Union“ (s. 16. TB Anlage 12) ausgesprochen.

Zuletzt forderte das Europäische Parlament die Kommission in seiner Entschließung Nr. 41 zum Arbeitsprogramm der Kommission für das Jahr 1997 auf, ein unabhängiges Datenschutzüberwachungsgremium zu schaffen.

Durch die im Juni 1997 in Amsterdam beschlossenen Änderungen des Vertrages über die Europäische Union und der Verträge zur Gründung der Europäischen Gemeinschaften wird diese offene Flanke jetzt geschlossen. Nach dem neuen Artikel 286 des am 2. Oktober 1997 als „Vertrag von Amsterdam“ verabschiedeten Unionsvertrages werden die Grundsätze der Richtlinie auf Datenverarbeitungen der Organe und Einrichtungen der Gemeinschaft angewendet und der Rat aufgefordert, auf Vorschlag der Kommission eine europäische Datenschutzaufsichtsbehörde zur Kontrolle der Gemeinschaftsstellen zu schaffen. Wörtlich lautet die Vorschrift:

„(1) Ab 1. Januar 1999 finden die Rechtsakte der Gemeinschaft über den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und dem freien Verkehr solcher Daten auf die durch diesen Vertrag oder auf der Grundlage dieses Vertrages errichteten Organe und Einrichtungen der Gemeinschaft Anwendung.

(2) Vor dem in Absatz 1 genannten Zeitpunkt beschließt der Rat gemäß dem Verfahren des Artikels 251 die Errichtung einer unabhängigen Kontrollinstanz, die für die Überwachung der Anwendung solcher Rechtsakte der Gemeinschaft auf die Organe und Einrichtungen der Gemeinschaft verantwortlich ist, und erläßt erforderlichenfalls andere einschlägige Bestimmungen.“

Zur Errichtung der in der Vorschrift genannten unabhängigen Kontrollinstanz hat die Kommission den Entwurf einer Verordnung ausgearbeitet (Draft Proposal for a Regulation of the European Parliament and the Council on the protection of individuals with regard to the processing of personal data by the institutions and bodies of the European Community and on the free movement of such data). Der Entwurf wurde im März und im Juni vergangenen Jahres seitens der Datenschutzgruppe nach Artikel 29 (s. o. Nr. 2.2) beraten, seine Verabschiedung durch den Rat steht noch aus.

2.4 Die Konferenz der Datenschutzbeauftragten der Europäischen Union

Auf der Frühjahreskonferenz der unabhängigen europäischen Datenschutzbehörden (s. auch **Anlage 28**) am 24. und 25. April 1997 in Wien wurden hauptsächlich Datenschutzprobleme mit Europabezug, insbesondere aus dem Bereich der sog. Dritten Säule des Vertrages über die Europäische Union (EUROPOL und Schengen) beraten. Einen weiteren Beratungsschwerpunkt bildete das Konzept der „datenschutzfördernden Technologien“, das mittlerweile unter dem Kürzel PET (Privacy Enhancing Technologies) bekannt ist (siehe auch Nr. 8.5 und **Anlage 11** dazu). Der niederländische Datenschutzbeauftragte berichtete über einen Feldversuch in sieben großen Krankenhäusern seines Landes zum Einsatz von PET bei der Führung elektronischer Krankengeschichten mit dem Ziel, die Privatsphäre der Patienten maximal zu schützen. Die französischen Kollegen berichteten über die Bemühungen einer Nutzbarmachung von PET zur Aktualisierung der Krankengeschichte von Aids-Patienten. Die Konferenz beschloß, eine europaweite Übersicht über PET-Anwendungen zu erarbeiten und den Einsatz dieser neuen Datenschutztechnologie in Informationssystemen zu fördern.

Auf der Konferenz vom 23. und 24. April 1998 in Dublin wurde neben EUROPOL (s. Nr. 11.4), Schengen (s. Nr. 11.5) und dem Zollinformationssystem – ZIS – (s. Nr. 13.5) das europäische daktyloskopische Fingerabdrucksystem zur Identifizierung von Asylbewerbern – EURODAC – (s. Nr. 5.7) behandelt. Ferner wurde die Umsetzung von Artikel 9 der EG-Datenschutzrichtlinie intensiv diskutiert, der die Verarbeitung personenbezogener Daten in ihrem Verhältnis zur Meinungsfreiheit regelt. Erneut wurden die strengeren Vorgaben der Richtlinie im Verhältnis zu manchen nationalen Rechten deutlich. So gilt im deutschen Recht derzeit nach § 41 BDSG für die Medien eine weitgehende Freistellung, während die Richtlinie für sie grundsätzlich in vollem Umfang gilt. Die Mitgliedstaaten können nach Artikel 9 der Richtlinie künftig Ausnahmen nicht mehr pauschal, sondern nur noch insoweit zulassen, als dies zum Ausgleich mit der Pressefreiheit erforderlich ist. Für weiteren Beratungsstoff sorgten aktuelle Probleme des Internet wie Marketing im Internet und Anforderungen an die Herstellung von Internetsoftware.

3 Deutscher Bundestag

3.1 Datenschutzordnung für den parlamentarischen Bereich

Der zuletzt in meinem 16. TB (Nr. 35, dort Nr. 1) angesprochene Entwurf einer **Datenschutzordnung des Deutschen Bundestages** ist auch in der abgelaufenen 13. Wahlperiode nicht verabschiedet worden. Auf Landesebene sind dagegen zu den von mir bereits vor zwei Jahren genannten Datenschutzordnungen für die Landtage in Hessen und Rheinland-Pfalz inzwischen auch Datenschutzordnungen für die Bremische Bürgerschaft und für den Landtag in Schleswig-Holstein hinzugekommen.

Der Geschäftsordnungsausschuß des Deutschen Bundestages hatte mich noch gegen Ende der 13. Wahlperiode gebeten, ihn bei der Überarbeitung und Aktualisierung des seit längerem vorliegenden Entwurfs zu unterstützen. In meiner Stellungnahme an den Geschäftsordnungsausschuß des 14. Bundestages habe ich insbesondere empfohlen, entsprechend dem BDSG eine Zweckbindungsregelung für personenbezogene Daten, die einem Berufs- oder besonderen Amtsgeheimnis unterfallen, und eine Regelung über Schadensersatzleistungen aufzunehmen. Darüber hinaus habe ich u. a. Vorschläge unterbreitet, die darauf abzielen, die Datenschutzordnung des Deutschen Bundestages an die Vorgaben der Europäischen Datenschutzrichtlinie 95/46/EG anzupassen.

Ich würde es begrüßen, wenn der Deutsche Bundestag in dieser Wahlperiode eine Datenschutzordnung für seine parlamentarische Tätigkeit beschließen würde.

3.2 Kaufinteressenten nicht mehr in Bundestags- und Bundesratsdrucksachen genannt

Nach § 64 Abs. 2 Bundeshaushaltsordnung (BHO) dürfen Grundstücke des Bundes, die erheblichen Wert oder besondere Bedeutung haben und deren Veräußerung im Haushaltsplan nicht vorgesehen ist, grundsätzlich nur mit Einwilligung des **Bundestages** und des **Bundesrates** veräußert werden. Ist die Zustimmung nicht eingeholt worden, so sind Bundestag und Bundesrat alsbald von der Veräußerung zu unterrichten. Bis zur Verabschiedung des Bundeshaushaltsplans 1998 wurden die für die Entscheidung oder Unterrichtung des Parlaments maßgeblichen Angaben in Bundestags- und Bundesratsdrucksachen abgedruckt. Hierzu zählten neben dem Kaufpreis und dem beabsichtigten Verwendungszweck des Grundstücks u. a. die Kaufinteressenten oder Erwerber.

Weil hiervon auch natürliche Personen betroffen waren, hatte mich das BMF um Stellungnahme zu den Datenübermittlungen an Bundestag und Bundesrat gebeten. In meiner Antwort habe ich dargelegt, daß die bisherige Praxis den Vorgaben des § 64 Abs. 2 BHO zwar zu entsprechen scheine; es komme allerdings darauf an, ob es erforderlich sei, dem Bundestag und dem Bundesrat auch die Kaufinteressenten oder die Erwerber namentlich zu benennen. Datenschutzrechtlich problematisch sei deren Angabe in den Bundestags- und Bundesratsdrucksachen aber auch, weil diese Drucksachen von jedermann bezogen werden könnten und darin enthaltene personenbezogene Daten damit letztlich allgemein zugänglich seien. Die Kaufinteressenten und Erwerber von Grundstücken brauchten hingegen nicht damit zu rechnen, daß andere als die für die Veräußerung zuständigen Personen Kenntnis von ihren mitgeteilten Daten erhalten. Insoweit ergebe sich ein unberechtigter Eingriff in ihr informationelles Selbstbestimmungsrecht. Ich habe angeregt, andere Verfahrenswege zu prüfen. So könnte es m.E. genügen, Bundestag und Bundesrat detailliert mit Ausschußdrucksachen zu unterrichten.

Außerdem habe ich auf einen vergleichbaren Fall hingewiesen, in dem die öffentliche Bekanntmachung der Namen natürlicher Personen in Parlamentsdrucksachen auf meine Bedenken hin eingestellt wurde (s. 14. TB Nr. 18.1). Damals wurden die Namen durch Schlüsselnummern ersetzt. Die notwendige Information der gesetzgebenden Körperschaften wurde mit Hilfe eines Schlüsselverzeichnisses für die Parlamentsmitglieder sichergestellt. Diese Lösung böte sich auch hier an.

Nach Mitteilung des Sekretariats des Haushaltsausschusses des Bundestages sowie des Sekretärs des Finanzausschusses des Bundesrates und des Leiters des dortigen Parlamentsdienstes konnte allerdings – so das BMF – nach damaliger Rechtslage zunächst nicht auf einen Abdruck der Angaben in den Drucksachen verzichtet werden, da alle Abgeordneten und die Mitglieder des Bundesrates ausreichend zu informieren waren. Wenig später wurde jedoch auf Vorschlag des BMF zur Beschleunigung des parlamentarischen Zustimmungsverfahrens bei Grundstücksveräußerungen und aus datenschutzrechtlichen Gründen folgende Regelung als Haushaltsvermerk in den Bundeshaushaltsplan 1998 (Kap. 08 07 Tit. 131 01 lfd. Nr. 1.05) aufgenommen: Grundstücke des Bundes, die erheblichen Wert oder besondere Bedeutung haben und deren Veräußerung im Haushaltsplan nicht vorgesehen ist, dürfen in Abweichung von § 64 Abs. 2 BHO mit Einwilligung des **Haushaltsausschusses des Bundestages** und des **Finanzausschusses des Bundesrates** veräußert werden, soweit nicht aus zwingenden Gründen eine Ausnahme hiervon geboten ist. Ist die Zustimmung nicht eingeholt worden, so sind wiederum auch allein der Haushaltsausschuß des Bundestages und der Finanzausschuß des Bundesrates alsbald von der Veräußerung zu unterrichten.

Damit beschränkt sich der Kreis der Empfänger der für die Veräußerung maßgeblichen Daten nunmehr auf die Personen, die sich im parlamentarischen Raum mit den Grundstücksveräußerungen im einzelnen zu befassen haben. Außerdem werden die Angaben nicht mehr in Bundestags- und Bundesratsdrucksachen, sondern nur noch in nicht öffentlichen Ausschußdrucksachen festgehalten. Datenübermittlungen an unbeteiligte Dritte sind damit ausgeschlossen. In Zusammenarbeit mit dem BMF konnte so eine Lösung gefunden werden, die sowohl datenschutzrechtlichen Interessen als auch den Belangen eines beschleunigten Verfahrens Rechnung trägt.

4 Auswärtiger Dienst

4.1 Überflüssige Bonitätsprüfungen

Im 16. TB (Nr. 4.2.1) habe ich Probleme bei der Erteilung von Visa an ausländische Gäste aufgezeigt. Insbesondere hielt ich eine erneute Überprüfung der Identität und Bonität eines deutschen Gastgebers, der eine Verpflichtungserklärung nach § 84 AuslG vorgelegt hat, durch die jeweils zuständige deutsche Vertretung im Ausland jedenfalls dann für überflüssig, wenn die Ausländerbehörde die Überprüfung bereits vorgenommen und dies auf der Verpflichtungserklärung bescheinigt hat. Das AA teilt grundsätzlich meine Auffassung.

Leider bestand dennoch in einigen Fällen für verärgerte Gastgeber, die bei der Ausländerbehörde eine Verpflichtungserklärung abgegeben hatten und deren Identität und Bonität von dort geprüft und bescheinigt worden war, Anlaß, sich bei mir zu beschweren, weil einige Auslandsvertretungen weiterhin Bescheinigungen (z. B. über die Höhe des Einkommens und des Vermögens) verlangt hatten.

Das AA hat mir bestätigt, daß in diesen Fällen eine erneute Prüfung durch die Auslandsvertretung regelmäßig nicht erforderlich ist. Ich habe das AA daraufhin gebeten sicherzustellen, daß bei allen deutschen Auslandsvertretungen künftig nach dieser bürgerfreundlichen und datenschutzgerechten Regelung verfahren wird (s. auch Nr. 5.2.2).

4.2 Familienzusammenführung deutsch-ausländischer Paare und Ermittlungen bei Verdacht auf sog. Scheinehe

Im Berichtszeitraum haben mich mehrere Bürgerinnen und Bürger gebeten, die Ermittlungstätigkeit deutscher Auslandsvertretungen in den Fällen datenschutzrechtlich zu überprüfen, in denen der ausländische Ehepartner ein Einreisevisum beantragt hatte und die Auslandsvertretung dem Verdacht nachging, die Ehe sei nur zu dem Zweck geschlossen worden, dem Antragsteller eine Aufenthaltserlaubnis zu verschaffen.

Ich habe die mit solchen Ermittlungen verbundenen datenschutzrechtlichen Probleme mit dem AA erörtert. Das AA hat hierzu ausgeführt, daß es im Rahmen der Ermittlungen bei Scheineheverfahren nach § 92 Abs. 2 Nr. 2 AuslG zulässig sei, personenbezogene Daten des Antragstellers für ein Visum nach § 75 Abs. 1 i.V.m. § 63 Abs. 3 AuslG zu erheben. Eine Mitwirkungspflicht des ausländischen Ehepartners ergebe sich aber auch aus § 70 Abs. 1 AuslG. Es liege im Ermessen der zuständigen Auslandsvertretung, den Sachverhalt durch Anforderung entsprechender Nachweise und ggf. in einer mündlichen Befragung aufzuklären. Hierzu könnten im Einzelfall auch Fragen zu den Umständen der Eheschließung gehören. Ein erheblicher Altersunterschied zwischen den Eheleuten könne z. B. ein Indiz dafür sein, daß eine sog. Scheinehe vorliege. Wegen der hohen Zahl von Mißbrauchsfällen sei es – auch im Interesse redlicher Antragsteller – erforderlich, die näheren Umstände der Eheschließung zu ermitteln; hierbei seien die gesellschaftlichen Besonderheiten des jeweiligen Gastlandes zu berücksichtigen. Fragen, die die Privatsphäre der Betroffenen berühren, seien dabei leider unvermeidbar. In einigen Fällen müsse die Auslandsvertretung zudem die Echtheit und inhaltliche Richtigkeit vorgelegter Urkunden über Vertrauensanwälte verifizieren lassen. In den vergangenen Jahren habe sich herausgestellt, daß ein großer Teil dieser Unterlagen gefälscht oder inhaltlich falsch gewesen sei. Ihre vorbehaltlose Anerkennung im deutschen Rechtsverkehr sei daher nicht möglich gewesen. Das AA betont, daß personenbezogene Daten stets in Kenntnis und mit Zustimmung der Betroffenen geprüft und übermittelt würden.

Der Argumentation des AA kann ich mich nicht verschließen. Mit dem AA besteht Einvernehmen darüber, daß Fragen zum privaten Lebensbereich nur insoweit zulässig sind, als es im Einzelfall zur Aufklärung des entscheidungserheblichen Sachverhalts zwingend erforderlich ist. Hinsichtlich der Bedeutung eines erheblichen Altersunterschiedes zwischen den Eheleuten stimme ich zwar mit dem AA überein, daß er ein Indiz für eine sog. Scheinehe sein kann. Aber erst das Zusammentreffen mit anderen Begleitumständen, wie z. B. fehlende sprachliche Verständigungsmöglichkeit oder ein getrennter Wohnsitz, kann die Annahme einer rechtsmißbräuchlichen Eheschließung nahelegen. Dies rechtfertigt dann auch entsprechende Nachfragen durch die Auslandsvertretung. Eine Befragung zum Sexualverhalten ist dabei auch nach Auffassung des AA nicht zulässig.

Wenngleich dieses Ergebnis aus meiner Sicht nicht ganz befriedigt, muß ich den Auslandsvertretungen diese Datenerhebungen zugestehen, damit sie einerseits Mißbrauchsfälle aufdecken und andererseits redlichen Antragstellern den Aufenthalt in der Bundesrepublik Deutschland ermöglichen können.

5 Innere Verwaltung

5.1 Protokollierung im Ausländerzentralregister

Im Sommer 1997 bin ich durch einen Landesbeauftragten für den Datenschutz darauf aufmerksam gemacht worden, daß eine Ausländerbehörde, die selbst noch keinen automatisierten Zugriff auf das Ausländerzentralregister (AZR) besaß, sich bei ihren Auskunftsersuchen an das AZR einer Grenzschutzstelle bedient hat, um Auskünfte aus dem Register schnell zu erhalten. Die Grenzschutzstelle, die für dieses Verfahren bereits zugelassen war, hat hierzu „im Wege der Amtshilfe“ und unter Angabe des unrichtigen Verwendungszwecks „grenzpolizeilicher Schutz“ Daten ausschließlich zur Weitergabe an die Ausländerbehörde abgerufen. Damit hat sie gegen § 10 Abs. 1 i.V.m. § 22 Abs. 4 Ausländerzentralregistergesetz (AZR-Gesetz) und § 8 Abs. 3 AZRG-Durchführungsverordnung (AZRG-DV) verstoßen.

Ich habe daraufhin erstmals seit Inkrafttreten des AZR-Gesetzes ein datenschutzrechtliches Kontrollverfahren eingeleitet und nach § 16 Abs. 2 AZRG-DV die Regi-

sterbehörde gebeten, die von den beteiligten Behörden eingegebenen und abgerufenen Daten nicht – wie vorgesehen – sechs Monate nach ihrer Entstehung zu löschen, sondern sie bis zum Abschluß des Kontrollverfahrens vorzuhalten. Gleichzeitig hat das BMI das zuständige Grenzschutzpräsidium angewiesen zu veranlassen, daß die fragliche Grenzschutzstelle in Zukunft keine Daten mehr für die Ausländerbehörde abruft. Damit hat das BMI die vorausgegangene rechtliche Bewertung des Grenzschutzpräsidiums, das darin zunächst keinen Verstoß gegen Vorschriften des AZR-Gesetzes sah, korrigiert.

Im Rahmen meiner Kontrolle habe ich festgestellt, daß der Umfang der Aufzeichnungen beim AZR den Vorgaben des § 13 AZR-Gesetz entspricht, die Registerbehörde durch systemtechnische Vorkehrungen eine Vielzahl möglicher Mißbrauchsfälle ausschließt und ihrer Pflicht nach § 16 Abs. 1 Satz 2 AZRG-DV, sich durch regelmäßige Kontrollen von der ordnungsgemäßen Funktion des Verfahrens zu überzeugen, nachkommt. Ich habe mich zudem im Rahmen einer technischen Demonstration davon überzeugen können, daß keine Grenzschutzstelle in der Lage ist, eine Ausländerbehörde zu simulieren und an ihrer Stelle Direkteingaben in das Register vorzunehmen. Verhindert wird dies durch programmtechnische Vorkehrungen, die sicherstellen, daß eine Grenzschutzstelle im AZR-Verfahren nur auf solche Dialogmasken (eine Dialogmaske ist einem Vordruck vergleichbar, mit dem z. B. Anfragen gestellt werden) zugreifen kann, die den speziellen Aufgaben des Grenzschutzes entsprechen. So ist eine Ersteinspeicherung von Daten durch den Grenzschutz in das AZR nur möglich, wenn sie im Zusammenhang mit den Fällen des § 2 Abs. 2 Nr. 3 bis 6 AZR-Gesetz steht. Diese Anlässe sind unveränderbar in der Dialogmaske für den Grenzschutz vorgegeben. Desweiteren bin ich der Frage nachgegangen, ob Auffälligkeiten im Vergleich mit anderen Grenzschutzstellen erkennbar waren, die Rückschlüsse auf den Umfang der „Amtshilfe“ für die Ausländerbehörde zugelassen hätten. Es hat sich gezeigt, daß wegen der Vielzahl der Datenübermittlungen entsprechende Auswertungen der Protokollaufzeichnungen durch die Registerbehörde kaum möglich sind. Auch Erfahrungswerte, die Aufschluß darüber bieten könnten, wieviele Datenübermittlungen an eine Grenzschutzstelle als durchschnittlich angesehen werden könnten, gibt es bei der Registerbehörde nicht. Ich habe es begrüßt, daß sich das BMI nach Abschluß meiner Kontrolle meinen Bewertungen in vollem Umfang angeschlossen und die Grenzschutzpräsidien sowie die Grenzschutzdirektion angewiesen hat, in ihrem Bereich sicherzustellen, daß keine Datenanfragen und Datenübermittlungen für andere Behörden stattfinden.

5.2 Ausländerrecht

5.2.1 Allgemeine Verwaltungsvorschriften zum Ausländergesetz

Nach § 104 AuslG erläßt das BMI mit Zustimmung des Bundesrates allgemeine Verwaltungsvorschriften zu diesem Gesetz und den auf Grund dieses Gesetzes erlassenen Rechtsverordnungen. Seit einigen Jahren, zuletzt in meinem 15. TB Nr. 35.1, habe ich diese Vorschriften, die u. a. die Datenschutzbestimmungen der §§ 75 ff. AuslG näher regeln sollen, wiederholt angemahnt. Das BMI hat im Jahr 1997 erstmals einen umfangreichen Entwurf der Verwaltungsvorschriften erarbeitet und mich frühzeitig an den Beratungen beteiligt. Ich habe in zahlreichen Kontakten mit dem BMI erreichen können, daß die für den Datenschutz relevanten Vorschriften, insbesondere über die Erhebung personenbezogener Daten, die Übermittlung an Ausländerbehörden sowie über die Verfahren bei erkennungsdienstlichen Maßnahmen, weiter präzisiert worden sind. Alles in allem entspricht der Entwurf der Verwaltungsvorschriften weitgehend meinen Empfehlungen.

Besonderen Wert habe ich auch auf eine datenschutzfreundliche Ausgestaltung der allgemeinen Verwaltungsvorschriften zu den §§ 82 und 84 AuslG gelegt, in denen das Verfahren bei Abgabe einer Verpflichtungserklärung für die Fälle näher geregelt wird, in denen sich eine Person gegenüber der Ausländerbehörde oder einer Auslandsvertretung verpflichtet hat, für eine bestimmte Zeit die Kosten für den Lebensunterhalt eines von ihr eingeladenen Ausländers zu tragen (Näheres s. u. Nr. 5.2.2).

Die Bundesregierung hat zwar in der vorherigen Legislaturperiode die allgemeinen Verwaltungsvorschriften abschließend behandelt, konnte aber die erforderliche Zustimmung des Bundesrates nicht herbeiführen. Ich hoffe, daß diese für die Praxis wichtigen Vorschriften in der neuen Legislaturperiode baldmöglichst erlassen werden.

5.2.2 Bonität des Gastgebers

Bereits in meinem 16. TB (Nr. 4.2.1) habe ich ausführlich über die Verfahrensweisen zur Prüfung der Bonität eines Gastgebers in der Praxis der Auslandsvertretungen und der Ausländerbehörden berichtet. Ausgangspunkt ist, daß die für die Visaerteilung zuständigen deutschen Auslandsvertretungen im Einzelfall prüfen, ob die für die Erteilung eines beantragten Besuchervisums erforderlichen Voraussetzungen oder ob Versagungsgründe vorliegen. Ein Versagungsgrund liegt z. B. vor, wenn der Ausländer seinen Lebensunterhalt während seines Aufenthaltes nicht aus eigenen Mitteln bestreiten kann. Das kann einem eingeladenen ausländischen Gast erspart werden, indem der Gastgeber gegenüber der Ausländerbehörde im Inland oder gegenüber der deutschen Auslandsvertretung eine sog. Verpflichtungserklärung nach § 84 AuslG abgibt (s. auch Nr. 4.1). Dabei gibt er Einkommens-, Vermögens- und Wohnverhältnisse sowie weitere persönliche Daten Dritten bekannt, was ich auch in meinem 16. TB (Nr. 4.2.1) – wie bereits seit mehreren Jahren gegenüber dem BMI – moniert habe.

Inzwischen liegt eine Neufassung der „Hinweise zur Verwendung des bundeseinheitlichen Formulars der Verpflichtungserklärung“ vor, die das BMI auf der Grundlage des Entwurfs zur Novellierung der Verwaltungsvorschriften zum AuslG erarbeitet hat. An der hierzu vom BMI durchgeführten Ressortabstimmung habe ich mitgewirkt. Meine Änderungswünsche, die darauf

zielten, eine Offenlegung von Daten aus dem Bereich der persönlichen Lebensverhältnisse gegenüber Dritten ohne Vorliegen eines sachlichen Grundes zu unterlassen, sind weitgehend in der Neufassung berücksichtigt worden. Ich begrüße es nachdrücklich, daß künftig auf Detailangaben zu Einkommens-, Vermögens- und Wohnverhältnissen des Gastgebers verzichtet wird. Bei seiner Neuauflage ist nach Angaben des BMI in dem Vordruck an Stelle des bisher auszufüllenden Feldes zu diesen Angaben ein Leerfeld vorgesehen. Bis zur Auslieferung des neuen Formblattes an die Ausländerbehörden soll nach Mitteilung des BMI in den Bundesländern bereits entsprechend verfahren und auf die Angabe der Einkommens-, Vermögens- und Wohnverhältnisse des Gastgebers im Vordruck verzichtet werden.

Nicht berücksichtigt wurde dagegen meine Empfehlung, auf die Angaben zu Beruf und Arbeitgeber des Gastgebers zu verzichten. Das BMI sieht darin weiterhin ein notwendiges Kriterium für die Bonitätsprüfung. Die Eignung dieser Daten für eine verläßliche Aussage im Rahmen der Bonitätsprüfung ist für mich nach wie vor zweifelhaft. Ich habe starke Bedenken, diese Angaben durch die Eintragung in das Formular auch Dritten gegenüber bekannt zu geben. Ebenfalls unberücksichtigt blieb meine Anregung darauf zu verzichten in den Fällen, in denen der Gastgeber Sozialhilfe bezieht, regelmäßig im Feld „Bemerkungen“ einzutragen, daß gegen die Einreise des Ausländers keine Bedenken bestehen. Diese Form der Eintragung, die sonst nicht vorgenommen wird, führt meines Erachtens dazu, daß ein Kenner des Verfahrens erfährt, daß der Gastgeber Sozialhilfe bezieht.

5.3 Machbarkeitsstudie zum Einsatz einer Smart-Card im Asylverfahren

Das BMI hat im Jahre 1997 eine „Machbarkeitsstudie zum Einsatz einer Smart-Card im Asylverfahren“ europaweit ausgeschrieben und den Zuschlag der deutschen Firma ORGA Consult GmbH erteilt. Anlaß für eine solche Studie war ein Vorschlag der „Bund/Länderarbeitsgruppe zur Harmonisierung der Verfahrensabläufe im Asylverfahren“, deren Federführung beim BAFl lag. Diese Arbeitsgruppe gelangte seinerzeit zu der Überzeugung, daß mit dem Einsatz einer Chipkarte das Ziel einer Harmonisierung der Verfahrensabläufe im Asylverfahren weitestgehend realisierbar sei. Mit Hilfe einer Machbarkeitsstudie sollte unter informationstechnologischen, rechtlichen, ökonomischen und sozio-systemischen Aspekten festgestellt werden, unter welchen Bedingungen die Verwendung einer Smart-Card im Asylverfahren sinnvoll sein könnte.

Von Anfang an, u. a. auch bei den Beratungen des Innenausschusses des Deutschen Bundestages zur Frage der Realisierung einer solchen Machbarkeitsstudie, habe ich erklärt, daß ich mich der Prüfung der Frage, inwieweit eine Chipkarte als Ausweis für Asylbewerber in der Bundesrepublik möglich sei, nicht verschließe. Ich habe mich dabei weder gegen eine Machbarkeitsstudie ausgesprochen, noch habe ich eine solche Chipkarte für Asylbewerber pauschal abgelehnt oder ihr undifferenziert zugestimmt. Gefordert habe ich allerdings, daß eine solche Chipkarte z. B. hinsichtlich der notwendigen Identifizierungsdaten wie auch bezüglich ihrer Fälschungssicherheit mit der gleichen Qualität ausgestattet sein müsse, wie der deutsche Personalausweis. Auch eine maschinelle Identifikation eines Asylbewerbers, etwa mit Fingerabdruck, der codiert in der Chipkarte gespeichert ist, müsse sicher erkennen lassen, daß es sich um den berechtigten Karteninhaber handele.

Im Verlauf der Durchführung der Machbarkeitsstudie habe ich das BAFl, dem wiederum die Koordinierung dieses Vorhabens oblag, wiederholt beraten. Dabei habe ich besonderen Wert darauf gelegt, daß in der Studie sowohl die asylrechtlichen als auch die datenschutzrechtlichen Aspekte in besonderer Weise gewürdigt werden. Ich habe mich zudem dafür eingesetzt, daß im Rahmen der Prüfung und Darstellung der datenschutzrechtlichen Probleme die Landesbeauftragten für den Datenschutz beteiligt werden. Aus unterschiedlichen Gründen haben sie von dieser Möglichkeit jedoch keinen Gebrauch gemacht.

Das BMI, dem die Machbarkeitsstudie im Sommer 1998 übergeben worden ist, hat mich darüber informiert, daß zunächst das BAFl mit einer genauen fachlichen Prüfung der Studie beauftragt sei. Dem Vernehmen nach liegt dem BMI das Ergebnis der Prüfung inzwischen vor. Ich gehe davon aus, daß es mich alsbald über seine weiteren Planungen zur Vorgehensweise unterrichten wird.

5.4 Kontrolle und Beratung des Bundesamtes für die Anerkennung ausländischer Flüchtlinge – BAFl – und seiner Außenstellen

5.4.1 Automatisierte Übermittlung von Fingerabdruckblättern vom BAFl an das BKA

Nach § 16 AsylVfG hat das BAFl die Identität eines Ausländers, der um Asyl nachsucht, durch erkennungsdienstliche Maßnahmen zu sichern, wenn er das 14. Lebensjahr vollendet hat und keine unbefristete Aufenthaltsgenehmigung besitzt. Dabei dürfen nur Lichtbilder und Abdrucke aller zehn Finger aufgenommen werden. Bei der Auswertung der Fingerabdruckblätter leistet das BKA Amtshilfe. Zur Beschleunigung der Übermittlung der Fingerabdruckblätter an das BKA hat das BAFl Ende 1996 seine Außenstellen mit dem sogenannten Telebildverfahren (Image-Transmission-System – ITS) ausgestattet. Es ersetzt die bisherige Zustellung der Fingerabdruckblätter an das BKA durch einen Kurierdienst.

Ich habe mir dieses Verfahren in der Praxis angesehen. Zur Übertragung der Fingerabdruckblätter an das BKA hat jede Außenstelle des BAFl einen leistungsstarken PC, einen Flachbettscanner und einen lokalen Drucker. Nach Abnahme der Fingerabdrucke wird das Fingerabdruckblatt an dem ITS-Arbeitsplatz gescannt und automatisiert an das BKA übertragen. Zur Gewährleistung der Datensicherheit dieses Verfahrens hat das BAFl die notwendigen Vorkehrungen nach § 9 BDSG getroffen. So wird z. B. durch softwaretechnische Maßnahmen sichergestellt, daß eine Übertragung nur an das BKA möglich ist.

Weiterhin ist positiv zu bewerten, daß nach der Übertragung die Daten nicht im ITS gespeichert bleiben und auch zu keiner Zeit eine Verknüpfung von ITS und dem vom BAFl betriebenen System ASYLON besteht. Die Auswertungsergebnisse des BKA lagen zum Zeitpunkt meiner Kontrolle dem BAFl in der Regel am nächsten Tag vor. Neu bei dem Telebild-Verfahren ist, daß die Auswertungsergebnisse zusätzlich und ohne Zeitverlust von einem besonders bestimmten Drucker in der jeweiligen Außenstelle ausgedruckt werden. Die Ausdrucke werden dem Einzelentscheider unverzüglich zugeleitet, damit er die Erkenntnisse des BKA bereits im Rahmen des Anhörungsverfahrens verwenden kann. Dies entspricht einer von mir wiederholt vorgetragenen Forderung.

Insgesamt halte ich das ITS-Verfahren für sachgerecht und erforderlich. Zu Hinweisen, daß Engpässe beim BKA die notwendige kurzfristige Bearbeitung der ITS-Anfragen zumindest zeitweise erschwert haben, hat das BMI erklärt, durch personelle und organisatorische Maßnahmen sei es inzwischen gelungen, sowohl die Fingerabdruckblätter zeitnah auszuwerten als auch das BAFl zügig über die Auswertungsergebnisse durch das BKA zu informieren.

5.4.2 Austausch von Asylbewerberdaten mit der Schweiz zum Zweck der Verwendung im Asylverfahren

Über den Austausch von Asylbewerberdaten zum Zweck der Verwendung im Asylverfahren zwischen dem BAFl und dem Schweizer Bundesamt für Flüchtlinge (BFF) und den in dieser Angelegenheit zwischen dem BMI und mir erzielten Verfahrenskompromiß hatte ich berichtet (s. 16. TB Nr. 5.4.2). Inzwischen habe ich mir im Rahmen einer Nachkontrolle einen Eindruck darüber verschafft, wie das BAFl das vereinbarte Verfahren in die Praxis umgesetzt hat. Ich konnte mich davon überzeugen, daß das BAFl in den Fällen, die bis zur Wiederaufnahme des Verfahrens auf der Basis der Absprache noch nicht beantwortet waren (sog. Altfälle), das BFF gebeten hat, für solche Auskunftsersuchen nachträglich die Einwilligungserklärung des Asylbewerbers in der vereinbarten Form zu übersenden. Ich halte es in diesem Zusammenhang für sachgerecht, daß das BAFl diejenigen Anfragen vernichtet hat, zu denen bis zum Ende des Jahres 1997 keine neue Einwilligungserklärung nachgereicht worden ist. Bei neuen Anfragen, die das BFF inzwischen auf der Grundlage des vereinbarten Musters gestellt hat, waren diese Erklärungen bis auf wenige Ausnahmen in der abgesprochenen Form entweder in deutscher, italienischer oder französischer Sprache beigefügt. Enthalten das AZR oder das beim BAFl geführte System ASYLON zu der von der Schweizer Behörde angefragten Person keinen Hinweis auf ein Asylverfahren, teilt das BAFl dem BFF mit einem Standardschreiben mit, daß *„unter diesen Personalien ein Asylverfahren nicht feststellbar“* ist. Führt die Abfrage des BAFl zu einem Eintrag in den vorerwähnten Datenbanken, legt das BAFl nach eingehender Identitätsprüfung fest, welche Unterlagen aus der Asylakte an das BFF übermittelt werden. Hierzu benutzt es ein Standardschreiben, aus dem im einzelnen ersichtlich ist, welche Unterlagen aus der Asylakte weitergegeben worden sind.

Die geschilderten Verfahrensweisen entsprechen der getroffenen Vereinbarung und auch meiner Empfehlung, den Datenaustausch mit der Schweiz sorgfältig zu dokumentieren.

5.4.3 Austausch von Asylbewerberdaten mit der Tschechischen Republik und mit Norwegen

Für den Austausch von Asylbewerberdaten mit der Schweiz habe ich einen Kompromiß in Form eines Einwilligungsverfahrens mit dem BMI erreichen können, über den ich in meinem 16. TB (Nr. 5.4.2) ausführlich berichtet habe. Dabei wurde auch abgesprochen, daß dieses Verfahren nicht ohne meine vorherige Konsultation auf weitere Staaten ausgedehnt werden soll.

Im Berichtszeitraum hat mich das BMI darüber informiert, daß es mit der Tschechischen Republik und mit Norwegen ebenfalls einen Austausch von Asylbewerberdaten auf der Grundlage der mit der Schweiz getroffenen Einwilligungslösung beabsichtige. Während ich gegen den Austausch der Daten mit der Tschechischen Republik keine Bedenken erhoben habe, da hier die für die Schweiz geltenden Verfahrensabsprachen analog angewandt werden, konnte ich dem Datenaustausch mit Norwegen zunächst nicht zustimmen. Der Grund dafür lag darin, daß Norwegen neben den üblichen Personalien dem BAFl auch noch Fingerabdruckdaten übermitteln wollte. Ich konnte zunächst nicht nachvollziehen, ob und in welcher Weise einem Asylbewerber in Norwegen erkennbar wird, daß seine Zustimmung zur Übermittlung seiner Daten stets auch einschließt, seine für ein dortiges Asylverfahren erhobenen Fingerabdruckdaten an das BAFl zu übermitteln und vom BKA auszuwerten. Das BMI hat mir inzwischen mitgeteilt, daß die zuständigen norwegischen Behörden die Einwilligungserklärung um einen Passus erweitert haben, der erkennen läßt, daß sich die vom Asylbewerber erteilte Zustimmung auch auf einen Registerabgleich von Fingerabdruckdaten im Ausland bezieht.

Unter dieser Voraussetzung und wenn das mit mir abgestimmte Muster der Einwilligungserklärung benutzt wird, habe ich gegen den Austausch personenbezogener Daten mit Norwegen keine Bedenken. Zusätzlich muß aber gewährleistet sein, daß das BKA die Fingerabdruckblätter so auswertet, daß – analog zur Umsetzung des Dubliner Übereinkommens – kein Bestandssatz gebildet wird, d. h. es bleiben keine Spuren in der AFIS-Datenbank. Das BMI hat mir dies bestätigt und mich zwischenzeitlich darüber unterrichtet, daß das BAFl die Übermittlung personenbezogener Daten mit Norwegen unter diesen Vorgaben zum 1. Dezember 1998 aufgenommen hat.

5.4.4 Abschiebung straffällig gewordener türkischer Asylbewerber – Deutsch-türkischer Briefwechsel –

Am 10. März 1995 trafen der deutsche und der türkische Innenminister eine Absprache zum Verfahren der Abschiebung von türkischen Staatsangehörigen, die sich an Straftaten im Zusammenhang mit der PKK und anderen Terrororganisationen in der Bundesrepublik beteiligt

haben. Ein wesentliches Element dieser Absprache ist, daß das BAFl bei der Prüfung der Frage, ob Abschiebungshindernisse nach § 53 AuslG (z. B. Gefahr für Leib, Leben oder Freiheit) bestehen, Hinweise auf die dem Betroffenen drohenden Risiken erhält, wenn Anhaltspunkte für die Zugehörigkeit des Asylbewerbers zu derartigen Organisationen bestehen. Um dies festzustellen, ist vorgesehen, über das BMI bei türkischen Behörden nachzufragen. Mit Blick auf die in § 7 AsylVfG normierte Erhebung personenbezogener Daten, die unter bestimmten Voraussetzungen auch bei ausländischen Behörden erfolgen kann, halte ich ein solches Verwaltungsverfahren für gerechtfertigt. Hervorzuheben ist, daß nach der Verfahrensabsprache in der Anfrage an die Türkei nicht erkennbar werden soll, ob es sich bei dem Betroffenen um einen Asylbewerber handelt. Dies entspricht auch dem Prinzip der in § 7 AsylVfG geforderten Vermeidung einer Beeinträchtigung überwiegender schutzwürdiger Interessen des Betroffenen.

Mein besonderes Interesse galt somit der vom BAFl auf der Grundlage der Absprache zur Sicherstellung eines einheitlichen Verfahrensablaufs erlassenen Dienstanweisung sowie der praktischen Durchführung des Verfahrens. Im Rahmen der Kontrolle einer Außenstelle des BAFl habe ich festgestellt, daß die dortige Bearbeitung den Vorgaben der Dienstanweisung entspricht. Keines der nach der Absprache in deutscher und türkischer Sprache zu verwendenden Formblätter trug einen Stempel des Bundesamtes, noch ließ ein sonstiger Hinweis erkennen, daß es sich bei der betroffenen Person um einen Asylbewerber handelt. Das Original der Anfrage geht dem BMI zusammen mit einem nach der Dienstanweisung vorgesehenen Anschreiben zu. Das BMI leitet es den türkischen Behörden mit der Frage zu, ob im Falle einer Abschiebung dem Betroffenen ein Strafverfahren oder eine Strafvollstreckung durch türkische Behörden droht. Die Zentrale des BAFl erhält von der bearbeitenden Außenstelle eine Kopie der Anfrage zur Registrierung und statistischen Erfassung. Da während meiner Kontrolle zu den von mir geprüften Fällen noch keine Antworten der türkischen Seite vorlagen, werde ich die sich daran anschließenden Bearbeitungsschritte des BAFl zu einem späteren Zeitpunkt erneut kontrollieren und darüber berichten.

5.4.5 Einsatz von Liaisonpersonal

Im Oktober 1998 habe ich den Einsatz deutschen Liaisonpersonals des BAFl im Ausland sowie den Einsatz ausländischen Liaisonpersonals im BAFl kontrolliert. Als Liaisonpersonal bezeichnet das BAFl die Mitarbeiter, die im Rahmen von bilateralen Verwaltungsvereinbarungen zu Partnerbehörden entsandt werden. Bei der Kontrolle führte ich nach Absprache mit dem BMI Einzelgespräche mit den Mitarbeitern des BAFl, die in Frankreich, Belgien und den Niederlanden eingesetzt sind, nicht – wie sonst üblich – am jeweiligen Arbeitsplatz vor Ort, sondern in der Zentrale des BAFl in Nürnberg.

5.4.5.1 Einsatz deutschen Liaisonpersonals des BAFl im Ausland

Der Aufgabenbereich und -umfang dieser Mitarbeiter ist in den Verwaltungsvereinbarungen festgelegt, die zwischen dem BMI bzw. dem BAFl und den ausländischen Behörden geschlossen wurden. Demnach besteht die Hauptaufgabe aller Liaisonbeamten in der Kontaktpflege und im Informationsaustausch zwischen der ausländischen Behörde, in die das Liaisonpersonal entsandt ist (Gastbehörde), und der Heimatbehörde. Dazu zählen insbesondere die Information der Gast- bzw. Heimatbehörde über die Gesetzgebung, das Asylverfahren und die Asylpraxis sowie die Beratung und Vermittlung in Fällen nach den Abkommen von Schengen/Dublin. Aus dem Wortlaut aller Vereinbarungen wird deutlich, daß das deutsche Liaisonpersonal Aufgaben des BAFl im Gastland wahrnehmen soll.

Das BAFl stellt seinem Liaisonpersonal grundsätzlich PCs zur Verfügung, für die Schutzmaßnahmen gegen Benutzung durch Unberechtigte sowie gegen Virenbefall durch Fremddisketten vorgesehen sind. Lediglich dem Liaisonpersonal in den Niederlanden wird die PC-Ausstattung durch die dortige Partnerbehörde zur Verfügung gestellt. Die Sicherungsmaßnahmen für die Informationstechnik richten sich in diesen Fällen nach den internen Vorgaben der niederländischen Gastbehörde.

Das BAFl übermittelt seine Aufträge an die Liaisonbeamten überwiegend per Fax, häufig telefonisch und auch auf normalem Postweg. In Belgien wird dem deutschen Liaisonbeamten ein separates Fax-Gerät in seinem Büro bereitgestellt, während in Frankreich und in den Niederlanden für das Liaisonpersonal keine gesonderten Fax-Geräte vorgehalten werden. Dort müssen die Geräte der jeweiligen Abteilung mitbenutzt werden, so daß das Personal dieser Abteilungen die Möglichkeit besitzt, per Fax übermittelte Schreiben einzusehen. Das BAFl hat seine Bereitschaft erklärt, zu prüfen, ob dem Liaisonpersonal eigene Fax-Geräte zur ausschließlichen Nutzung bereitgestellt werden können.

Die konkrete Aufgabenzuweisung erfolgt aus den Fachreferaten des BAFl, wenn es sich z. B. um Berichte allgemeiner Art, um Sachverhaltsaufklärungen in allgemeinen Rechtsfragen, um Gesetzesvorhaben des Gastlandes sowie um Nachfragen bei Anfragen nach Artikel 15 Dubliner Übereinkommen (DÜ), um Übernahmeersuchen oder um Reisewegbeschreibungen handelt.

Neben den auf Weisung des BAFl wahrzunehmenden Aufgaben erledigen die Liaisonbeamten auch Aufgaben, die durch – überwiegend telefonische – Anfragen anderer deutscher Behörden an sie herangetragen werden. Hierbei handelt es sich vor allem um Anfragen von deutschen Ausländerbehörden zu Ausländerangelegenheiten, von BGS-Dienststellen zu grenzüberschreitenden Asyl- und Ausländerangelegenheiten, von deutschen Auslandsvertretungen zu Aufenthalts-, Unterhalts- oder Visaangelegenheiten und von deutschen Verbindungsbeamten des Zolls und der Polizei im Ausland. Weitere anfragende Stellen sind deutsche Kriminalpolizeidienststellen und Stadtverwaltungen sowie deutsche Gerichte.

Über ihre Funktion als „Sprachmittler“ zwischen den deutschen und ausländischen Dienststellen hinaus beraten die Liaisonbeamten ihre jeweilige Gastbehörde in formaler und inhaltlicher Hinsicht insbesondere bei der Stellung von Übernahmeersuchen. Sie üben damit quasi

eine „Vorkontrolle“ bei der Prüfung der Frage aus, ob das Übernahmeersuchen Aussicht auf Erfolg hat. Die Liaisonbeamten erhalten auch Anfragen ausländischer Behörden des jeweiligen Gastlandes. Diese Anfragen sind zwar ausländerrechtlicher Natur, werden aber inhaltlich nicht von den Schengen/Dublin-Abkommen erfaßt.

Noch kann ich nicht erkennen, ob die Wahrnehmung aller genannten Aufgaben vom Inhalt der getroffenen Vereinbarungen getragen wird. Die Frage, ob das BAFl-Liaisonpersonal auch für Aufgaben eingesetzt werden darf, die entweder im Zuständigkeitsbereich anderer deutscher Behörden oder im ausschließlichen Zuständigkeitsbereich der jeweiligen Gastbehörde liegen (Stichwort „Funktionsdoppelung“), habe ich gegenüber dem BMI problematisiert. Ich möchte dabei insbesondere wissen, auf welcher Rechtsgrundlage die BAFl-Mitarbeiter in diesen Fällen tätig werden.

Einen direkten Zugang zu ausländischen Datenbanken haben die Liaisonbeamten grundsätzlich nicht. In der Regel erhalten sie Auskünfte aus diesen Datenbanken, indem ein ausländischer Kollege die Daten über seinen PC abruft oder er ihnen selbst den Zugriff von seinem Terminal aus gestattet.

Um Auskünfte aus den deutschen Datenbanken (AZR und ASYLON) zu erhalten, muß das Liaisonpersonal das Fachreferat des BAFl einschalten, da die Möglichkeit eines unmittelbaren Zugriffs für sie nicht besteht. Nach Abfrage des Registers werden die jeweiligen Ausdrucke erstellt und dem anfragenden Liaisonbeamten durch Fax übermittelt. Ich habe festgestellt, daß sich die Liaisonbeamten in den Niederlanden – mit Blick auf ihre bis zur Entscheidungsreife vorprüfende Tätigkeit im Rahmen der niederländischen Übernahmeersuchen – grundsätzlich die Ausdrucke aus ASYLON und dem AZR übersenden lassen. Werden sie bei dieser Aufgabenerledigung für die niederländische Behörde tätig, stellt dies eine Datenübermittlung an die ausländische Behörde dar. Eine Rechtsgrundlage für eine solche umfassende Datenübermittlung aus dem AZR an eine ausländische Stelle sieht das AZR-Gesetz jedoch nicht vor. Auch zu dieser Frage habe ich das BMI um Stellungnahme gebeten.

5.4.5.2 Einsatz ausländischen Liaisonpersonals in der Zentrale des BAFl

In der Zentrale des BAFl werden entsprechend dem Einsatz der deutschen Liaisonbeamten auch Angehörige ausländischer Partnerbehörden eingesetzt. Der Aufgabenbereich dieses Liaisonpersonals richtet sich ebenfalls nach den oben bereits erwähnten Vereinbarungen. Im Zeitpunkt der Kontrolle waren ein belgischer und ein niederländischer Liaisonbeamter im BAFl tätig. Die Aufgabenbereiche des belgischen Mitarbeiters sind gegenüber dem Inhalt der bilateralen Vereinbarungen erweitert worden. So nimmt er neben seiner Tätigkeit als Beschäftigter seiner Heimatbehörde bereits – wie ein vergleichbarer BAFl-Mitarbeiter – Aufgaben in der Koordinierungsstelle Schengen/Dublin des BAFl wahr. Dabei handelt es sich um die Bearbeitung der Anfragen nach Artikel 15 DÜ, die die belgische Seite an das BAFl richtet. In Anwendung der Funktionsdoppelungstheorie durch das BAFl ist er in das Verfahren wie folgt eingebunden worden:

Anfragen der belgischen Behörde werden zunächst auf Trefferfälle überprüft. Liegen solche vor, werden die Anfragen mit den entsprechenden Ausdrucken der AZR- und ASYLON-Abfragen dem belgischen Liaisonbeamten übergeben. Dieser wertet sie aus, übersetzt die aus seiner Sicht erforderlichen Informationen in die französische oder flämische Sprache und übermittelt sie nach Belgien.

Folgt man dem Gedanken der Funktionsdoppelung nicht, stellt bereits die Aushändigung der Ausdrucke eine Datenübermittlung in das Ausland dar, die in dieser Form nach dem AZR-Gesetz unzulässig ist. Dem belgischen Liaisonbeamten dürfen daher nur diejenigen personenbezogenen Daten ausgehändigt werden, die sonst zulässigerweise unmittelbar der belgischen Partnerbehörde übermittelt werden. Bis zum Abschluß der rechtlichen Klärung der Gesamtproblematik habe ich das BMI und das BAFl gebeten, sicherzustellen, daß dem belgischen Liaisonpersonal personenbezogene Daten aus den Datenbanken AZR und ASYLON nur in der Form zugänglich gemacht werden, wie dies zur Bearbeitung der Artikel 15 DÜ-Anfragen zulässig ist.

Allerdings war bei meiner Kontrolle bereits ein unmittelbarer Datenbankzugriff des Liaisonbeamten auf diese Datenbanken durch das BAFl zu Testzwecken eingerichtet. Eine solche Zugriffsmöglichkeit stellt ebenfalls eine Datenübermittlung in das Ausland dar, die insbesondere im Hinblick auf § 10 Abs. 4 AZR-Gesetz datenschutzrechtlich bedenklich ist. Ein Zugang des ausländischen Liaisonpersonals zu diesen Datenbanken wäre nur dann zulässig, wenn der oben angesprochenen Theorie der Funktionsdoppelung gefolgt werden kann. Ich habe das BAFl aufgefordert, diesen Testbetrieb unverzüglich einzustellen, was auch umgehend erfolgte.

Ohne eine Entscheidung zur Theorie der Funktionsdoppelung zu präjudizieren, sind datenschutzrechtliche Probleme beim Zugriff ausländischen Personals auf deutsche Datenbanken schon jetzt offensichtlich. Dies gilt z. B. für den Grundsatz, daß nur die für eine Aufgabenerledigung erforderlichen Daten zugänglich sein dürfen, oder für die Möglichkeit, daß ein Datenbankzugang dazu mißbraucht werden könnte, auch in anderen als den ursprünglich vorgesehenen Fällen Recherchen durchzuführen. Ein unbegrenzter Zugang des ausländischen Liaisonpersonals zu den deutschen Datenbanken birgt das Risiko, daß von ausländischen Behörden unter Umgehung des offiziellen Dienstweges das Liaisonpersonal im BAFl kontaktiert wird, um z. B. Auskünfte aus den Datenbanken zu erhalten, die sie sonst entweder gar nicht, nur im begrenzten Umfang oder nur nach Prüfung durch die jeweilige Facheinheit bekommen dürften. Daß diese Möglichkeit nicht von der Hand zu weisen ist, haben mir Liaisonbeamte des BAFl berichtet, die solchen Anfragen deutscher Behörden nicht entsprochen haben. Meine Bedenken begründen sich darin, daß nach § 18 AZR-Gesetz das BAFl über die größtmögliche Zugriffs-

berechtigung auf den Datenbestand des AZR verfügt, eine auf den Einzelarbeitsplatz zugeschnittene Berechtigung aber nicht möglich ist. Allerdings ermöglicht die in § 13 Abs. 1 AZR-Gesetz vorgeschriebene Protokollierung bei einem eventuellen Datenmißbrauch Zugriffe auf den Datenbestand des Registers nachzuvollziehen. Auch das System ASYLON bietet bei der Bearbeitung der Anfragen nach Artikel 15 DÜ Recherchemöglichkeiten, läßt zur Zeit aber keine Protokollierung zu. Im Gegensatz zum AZR ist es jedoch möglich, ein auf den konkreten Arbeitsplatz zugeschnittenes Berechtigungsprofil für Zugriffe in Form einer Bildschirmmaske zur Verfügung zu stellen. Mit dieser erhielte ein ausländischer Liaisonbeamter nur zu den Daten Zugang, die für die Beantwortung seiner Anfragen unbedingt erforderlich sind.

Wegen der Kürze der dem BMI für eine Äußerung zur Verfügung stehenden Zeit lag mir bei Redaktionsschluß dessen Stellungnahme zu meinem Kontrollbericht, insbesondere zur Frage der Funktionsdoppelungstheorie, noch nicht vor.

5.5 Warndateigesetz

Das BMI hat im Berichtszeitraum den Entwurf eines Artikelgesetzes vorgelegt, mit dem das AZR-Gesetz geändert und auch ein Gesetz zur Einrichtung einer Warndatei geschaffen werden sollte. Ziel dieses Gesetzentwurfs war es, die illegale Zuwanderung, das mißbräuchliche Asylbegehren und die Erschleichung von Sozialleistungen wirksam einzudämmen.

Im Verlauf der Ressortabstimmungen, aber auch in vielen öffentlichen Stellungnahmen, habe ich diese Gesetzesinitiative immer wieder kritisiert. Nach dem Entwurf sollten etwa die Daten desjenigen, der als Gastgeber eine Verpflichtungserklärung nach § 84 AuslG (s. auch Nr. 5.2.2) abgegeben hat, um einem eingeladenen Ausländer zu ermöglichen, sein Visum zu bekommen, unter bestimmten Voraussetzungen in einer sog. Warndatei gespeichert werden. Dies war in den Fällen vorgesehen, in denen der Ausländer bei der Beantragung seines Visums gefälschte oder verfälschte Dokumente vorgelegt oder nach seiner Einreise in die Bundesrepublik Deutschland einen Asylantrag gestellt hat. In beiden Fallkonstellationen kann man m. E. aber nicht den Gastgeber verantwortlich machen.

Gegen die Aufnahme personenbezogener Daten des Gastgebers in diese Warndatei habe ich erhebliche Bedenken geäußert. Dies gilt um so mehr, wenn der Gastgeber alle sich aus der Verpflichtungserklärung ergebenden Pflichten erfüllt und somit in optimaler Weise den staatlichen Erwartungen genügt.

In der abgelaufenen Legislaturperiode ist der Entwurf des Artikelgesetzes nicht mehr in die parlamentarischen Beratungen eingebracht worden. Es bleibt abzuwarten, ob und in welcher Form die neue Bundesregierung dieses Vorhaben aufgreifen wird.

5.6 Verwendung von Daten von Bürgerkriegsflüchtlingen

Von einem Landesdatenschutzbeauftragten erhielt ich Ende 1996 die Information, das BMI habe beim BAFl veranlaßt, eine Projektgruppe zur Datenerfassung einzurichten, die personenbezogene Daten von Bürgerkriegsflüchtlingen aus Bosnien-Herzegowina erfassen sollte. Die hierfür erforderlichen Daten würden von den Ausländerbehörden erhoben und über die jeweiligen Landesinnenministerien an die Projektgruppe weitergegeben werden. Dort sollten sie dann dazu genutzt werden, Mittel der EU und anderer Geldgeber für Wiederaufbau- und Rückführungsprojekte zur Förderung der freiwilligen Rückkehr dieses Personenkreises zu beschaffen. Durch einen anderen Hinweis erfuhr ich, daß das BMI die Innenressorts der Länder gebeten hat, die Daten der Bürgerkriegsflüchtlinge ohne deren Einwilligung an die Projektgruppe zu übermitteln.

Im Rahmen einer Kontrolle habe ich mir Anfang 1997 zunächst ein Bild über die Verfahrensabläufe von der Entgegennahme personenbezogener Daten bei der Projektgruppe bis zu einer Übermittlung an die deutsche Auslandsvertretung in Sarajewo machen können. Dabei habe ich festgestellt, daß die Projektgruppe entsprechend meinen vorausgegangenen Empfehlungen personell, technisch und organisatorisch von der eigentlichen Aufgabe des BAFl, Asylverfahren durchzuführen, getrennt worden ist. Da das BMI zunächst keine Vorgaben zur Struktur der Datenbank gegeben hatte, orientierte sich die Projektgruppe bei deren Aufbau hilfsweise an den vom Land Baden-Württemberg übermittelten Daten. Obwohl nur solche Daten erfaßt werden sollten, die erforderlich sind, um Fördermittel zu beantragen, habe ich festgestellt, daß in einzelnen Fällen auch andere Daten, z. B. die nur im Verkehr mit dem AZR zugelassene AZR-Nummer oder ein Hinweis auf ein früheres Asylverfahren, gespeichert wurden. Auf meine Empfehlung hin wurden solche Informationen umgehend gelöscht.

Die in der Datenbank gespeicherten Daten wurden darüber hinaus noch an die deutsche Botschaft in Sarajewo übermittelt, die im Zusammenwirken mit verschiedenen Organisationen (z. B. UNHCR) das sog. matching durchführte. Dabei wurde überprüft, ob die von den in der Bundesrepublik lebenden Bürgerkriegsflüchtlingen gegenüber den deutschen Ausländerbehörden gemachten Angaben mit den tatsächlichen Gegebenheiten in Bosnien-Herzegowina übereinstimmten: Hierbei handelt es sich beispielsweise um frühere Eigentums- oder Mietverhältnisse oder um den baulichen Zustand der Wohnung.

Ende 1997 habe ich die Projektgruppe erneut kontrolliert. Ich wollte vor allem prüfen, wie mit den von der deutschen Auslandsvertretung in Sarajewo an die Projektgruppe zurückübermittelten Daten umgegangen wird und wie sich die Datenbank entwickelt hat. Zum Zeitpunkt der Kontrolle waren in der Datenbank ca. 125 000 Datensätze von Bürgerkriegsflüchtlingen aus Bosnien-Herzegowina gespeichert. Ein erheblicher Teil der Länder war der Bitte des BMI nicht nachgekommen, die gewünschten Daten der Projektgruppe zu übermitteln. Die Daten der deutschen Auslandsvertretung gingen der Projektgruppe in Form sog. Evaluierunglisten zu, die das Ergebnis des sog. matchings, nämlich Informationen über die Bewohner der überprüften Wohnobjekte, deren baulichen Zustand und über die früheren Eigentums- und

Mietverhältnisse enthielten. Die Projektgruppe hat die personenbezogenen Datensätze, die sich auf die für eine mögliche Rückkehr in Frage kommenden Bügerkriegsflüchtlinge bezogen, mit den in der Datenbank gespeicherten Datensätzen verglichen. In den Fällen, in denen sie in der Datenbank einen Eintrag vorfand, hat sie einen Datenbankauszug gefertigt und diesen gemeinsam mit einer Kopie aus der entsprechenden Evaluierungsliste dem BMI zugeleitet. Dieses sollte die Daten über das jeweilige Landesinnenministerium den zuständigen Ausländerbehörden weitergeben. Bei den Datensätzen, die nicht in der Datenbank ermittelt werden konnten, lag die Vermutung nahe, daß sie der Projektgruppe von den Ländern nicht gemeldet worden waren. In diesen Fällen, so hatte das BMI entschieden, sollte die Projektgruppe durch eine Anfrage beim AZR *„den Aufenthalt in Deutschland bestätigen und die zuständige Ausländerbehörde bestimmen“*. Die Projektgruppe hat hierzu das AZR abgefragt und zwar im automatisierten Verfahren nach § 22 AZR-Gesetz, wobei der beim BAFl übliche Verwendungszweck „asylrechtliche Aufgabe“ angegeben wurde. Dies steht im deutlichen Gegensatz zu meiner ausdrücklichen Empfehlung, die Projektgruppe von den herkömmlichen asylverfahrensrechtlichen Aufgaben des BAFl zu trennen. Danach hätte der Projektgruppe lediglich eine Grunddatenauskunft nach § 14 AZR-Gesetz im nicht-automatisierten Verfahren zugestanden. Von einer förmlichen Beanstandung habe ich nur deshalb abgesehen, weil mir versichert wurde, meinen Empfehlungen zu entsprechen, falls solche Abfragen im AZR künftig wieder notwendig würden. Dies bedeutet, daß dann nur eine Grunddatenauskunft im nicht-automatisierten Verfahren eingeholt wird.

Im übrigen zeigte sich, daß wegen ausbleibender Datenübermittlungen aus den Ländern die ursprüngliche Zielsetzung der Datenbank nicht erreicht werden konnte. Mein Interesse gilt daher insbesondere der künftigen Nutzung der Datenbank. Ich habe das BMI Ende 1997 gebeten, mir mitzuteilen, wie die Zukunft der Projektgruppe und der Datenbank aussieht. Es hat mich dahingehend informiert, daß ein unmittelbarer Zugriff auf die Datenbank über das Netz inzwischen nicht mehr möglich ist, da die Daten auf einem externen Datenträger gespeichert sind, der unter Verschluß gehalten wird. Eine Entscheidung über den Zeitpunkt der Löschung der Datenbank soll nach vorhergehender Abstimmung mit den Ländern im Frühjahr 1999 herbeigeführt werden.

5.7 Europäisches daktyloskopisches Fingerabdrucksystem zur Identifizierung von Asylbewerbern (EURODAC)

In meinem 16. TB (Nr. 5.5) habe ich darüber berichtet, daß auf der Grundlage von Artikel 15 des Dubliner Übereinkommens über die Bestimmung des zuständigen Staates für die Prüfung eines in einem Mitgliedstaat der EU gestellten Asylantrages ein elektronisches System mit der Bezeichnung EURODAC eingerichtet werden soll. Innerhalb der Kommission wird eine Zentraleinheit eingerichtet, die dafür zuständig ist, im Namen der Mitgliedstaaten die zentrale Datenbank für die Fingerabdrucke von Asylbewerbern zu betreiben. Die Arbeiten an einem entsprechenden Konventionsentwurf sind im Berichtszeitraum intensiviert worden und inzwischen soweit fortgeschritten, daß die Beratungen vor dem Abschluß stehen. Noch in der ersten Jahreshälfte 1999 soll die Konvention durch den Rat beschlossen werden, die danach in das nationale Recht der jeweiligen Vertragsstaaten umzusetzen ist.

Im Verlauf der Beratungen wurde zwischen den Vertragsstaaten vereinbart, durch ein Zusatzprotokoll zur EURODAC-Konvention den Abgleich von Fingerabdrucken auf den Personenkreis illegal eingereister Ausländer auszudehnen. Hierbei soll zwischen den Ausländern unterschieden werden, die illegal an der Außengrenze oder in einem festgelegten grenznahen Raum des Mitgliedstaats angetroffen werden und denen, die sich illegal im Binnenland aufhalten. Der ersten Gruppe sollen stets Fingerabdrucke abgenommen und für einen festgelegten Zeitraum in EURODAC gespeichert werden. Den im Binnenland illegal angetroffenen Ausländern hingegen sollen Fingerabdrucke nur dann abgenommen werden, wenn Fakten vorliegen, die den Schluß rechtfertigen, daß diese Personen bereits in einem anderen Mitgliedstaat Asyl beantragt haben. Deren Fingerabdrucke werden lediglich mit EURODAC abgeglichen, nicht jedoch gespeichert. Eine Beschlußfassung des Rates über den Entwurf des Zusatzprotokolls wird ebenfalls im ersten Halbjahr 1999 angestrebt, so daß ein gemeinsames Inkrafttreten der Konvention und des Zusatzprotokolls möglich ist.

Der Verfahrensablauf nach der EURODAC-Konvention stellt sich bei Redaktionsschluß wie folgt dar:

Die Mitgliedstaaten nehmen unverzüglich nach Antragstellung jedem Asylbewerber oder jedem illegal an der Außengrenze oder im grenznahen Raum angetroffenen Ausländer die Fingerabdrucke ab und übermitteln diese an die Zentraleinheit, die über die technische Ausstattung zur Speicherung und zum Abgleich verfügt. Hervorzuheben ist, daß lediglich die Fingerabdrucke, eine von dem einspeichernden Mitgliedstaat vergebene Referenznummer und nur wenige Verfahrensdaten übermittelt werden. Das Ergebnis des automatisierten Abgleichs beschränkt sich darauf, daß mitgeteilt wird, ob diese Person bereits vorher in einem oder mehreren anderen Mitgliedstaaten einen Asylantrag gestellt hat. Die endgültige Identifizierung wird danach von dem anfragenden Mitgliedstaat nach Artikel 15 des Dubliner Übereinkommens in bilateraler Zusammenarbeit mit den betroffenen Mitgliedstaaten vorgenommen.

Neben meinen Bemühungen, den Datenumfang der Speicherung und Übermittlung auf das erforderliche Maß zu reduzieren, habe ich mich auch besonders dafür eingesetzt, daß die Konvention klare Definitionen hinsichtlich der **Rechte des Betroffenen** enthält. So enthält der Konventionsentwurf ausführliche Regelungen zu Auskunfts-, Berichtigungs- und Löschungsansprüchen des Betroffenen einschließlich ihrer gerichtlichen Durchsetzung in den Mitgliedstaaten sowie Regelungen zur Verantwortung der Mitgliedstaaten für die Verwendung der Daten. Die Rechte des Betroffenen sollen darüber hinaus durch die Einrichtung einer **Kontrollinstanz bei**

der Zentraleinheit und durch die Einbeziehung der nationalen Kontrollinstanz gewahrt werden. Bis zur Errichtung der unabhängigen Kontrollinstanz der Zentraleinheit wird eine gemeinsame Kontrollinstanz eingerichtet, die sich aus Vertretern der nationalen Datenschutz-Behörden eines jeden Mitgliedstaates zusammensetzt. Die in jedem Mitgliedstaat zu benennende unabhängige nationale Kontrollinstanz hat die Aufgabe, die Rechtmäßigkeit der Verarbeitung personenbezogener Daten durch den betreffenden Mitgliedstaat und die Übermittlung dieser Daten an die Zentraleinheit zu überwachen. Es ist davon auszugehen, daß diese Funktion in der Bundesrepublik Deutschland durch mich wahrgenommen wird.

Ich habe mich dafür eingesetzt, daß dem Betroffenen bei der Wahrnehmung seiner Rechte auf Berichtigung und Löschung von Daten Unterstützung und Beratung gewährt wird. Die Kontrolle, ob bei der Verarbeitung oder Nutzung dieser Daten durch die Zentraleinheit die Rechte des Betroffenen verletzt werden, obliegt der Kontrollinstanz der Zentraleinheit. Den Kontrollinstanzen sind für die Wahrnehmung ihrer Aufgaben umfangreiche Auskünfte zu erteilen, Zugriffe auf die gespeicherten Daten zu ermöglichen sowie Einsicht in alle relevanten Unterlagen und Akten und Zutritt zu allen Diensträumen zu gewähren.

Das Verfahren zum Abschluß der Konvention, des Zusatzprotokolls und der dazu zu erlassenden Durchführungsbestimmungen sowie des Ratifizierungsgesetzes, mit dem diese Regelungen in nationales Recht transformiert werden, werde ich aufmerksam weiter begleiten.

5.8 Rückübernahmeabkommen

Die Bundesregierung hat in den letzten Jahren zahlreiche Verträge mit anderen Staaten, u. a. mit Vietnam, Jugoslawien, Bosnien-Herzegowina, Marokko, Algerien, über die Rückübernahme von ausländischen Staatsangehörigen geschlossen, die keinen gültigen Aufenthaltstitel für die Bundesrepublik Deutschland besitzen. Diese Rückübernahmeabkommen enthalten Zweckbindungsregelungen für die zu übermittelnden Daten und Auskunftsrechte für die Betroffenen. Um eine reibungslose Rückführung zu ermöglichen, ist es notwendig, dem Empfängerstaat bestimmte Informationen zu geben. Die Verträge enthalten deshalb einen eigenen Datenschutzartikel, in dem die zur Durchführung des Abkommens zu übermittelnden Daten abschließend aufgezählt werden. Allerdings weiten die Protokolle zu den jeweiligen Abkommen diesen Datenumfang in vielen Fällen unverhältnismäßig aus, z. B. durch die Angabe von Gesundheitsdaten im Abkommen mit Jugoslawien. Unter dem Gesichtspunkt der Erforderlichkeit habe ich stets großen Wert darauf gelegt, daß die Datenübermittlungen im Zusammenhang mit Rückübernahmen so sparsam wie möglich erfolgen. So habe ich erreichen können, daß dies in den Fällen, in denen Daten über den im Abkommen festgelegten Rahmen hinaus erhoben bzw. übermittelt werden, nur mit einem ausdrücklichen Hinweis auf die Freiwilligkeit oder nur mit Einwilligung des Betroffenen erfolgen darf, z. B. im Abkommen mit Jugoslawien. Mit diesen Forderungen sehe ich mich auch im Einklang mit den Landesbeauftragten für den Datenschutz, die die Umsetzung der Übereinkommen und der Durchführungsprotokolle durch die zuständigen Landesbehörden im Rahmen ihrer Zuständigkeiten beratend und kontrollierend begleiten.

5.9 Unterlagen des Staatssicherheitsdienstes der ehemaligen DDR

5.9.1 Verwendung von Stasi-Unterlagen für Zwecke parlamentarischer Untersuchungsausschüsse

In meinem 16. TB (Nr. 5.9.1) habe ich über die Verwendung von Stasi-Unterlagen für Zwecke parlamentarischer Untersuchungsausschüsse berichtet. Zwar dürfen Stasi-Unterlagen nach § 22 StUG auch zu Zwecken der Beweiserhebung durch parlamentarische Untersuchungsausschüsse verwendet werden, allerdings nur, wenn der Untersuchungsauftrag in Übereinstimmung mit den in § 1 StUG aufgeführten Gesetzeszwecken steht. Dies war seinerzeit nicht gegeben. Ich habe daher der Bundesregierung im Hinblick auf mögliche künftige Anforderungen von Stasi-Unterlagen durch Untersuchungsauschüsse empfohlen, im Rahmen ihrer Rechtsaufsicht nach § 35 Abs. 5 Satz 3 StUG ein Rechtsverständnis der maßgeblichen Vorschriften des Stasi-Unterlagen-Gesetzes sicherzustellen, das Zweifel an einer verfassungskonformen Rechtsanwendung ausschließt.

In ihrer Stellungnahme zu meinem 16. TB hat die Bundesregierung ausgeführt, daß nach einem Beschluß des Landgerichts Kiel die Rechte der Betroffenen aus Artikel 10 Abs. 1 GG (Brief-, Post- und Fernmeldegeheimnis) bezüglich der durch das Abhören des Fernmeldeverkehrs gewonnenen Stasi-Unterlagen Vorrang gegenüber dem Aufklärungsinteresse eines parlamentarischen Untersuchungsausschusses hätten. Das Recht eines Betroffenen aus Artikel 10 Abs. 1 GG werde durch § 22 StUG nicht beschränkt, soweit der Untersuchungsgegenstand nicht mit den in § 1 StUG bestimmten Gesetzeszwecken übereinstimme. Insoweit greife das Verbot des § 5 StUG, Unterlagen zum Nachteil von Stasi-Opfern zu verwenden, ein. Die Bundesregierung gehe davon aus, daß der BStU diese Rechtsprechung zur Grundlage seiner Entscheidungen bei eventuellen künftigen Ersuchen machen werde. Desweiteren sei fraglich, ob es nochmals zu derartigen Anfragen kommen werde, da zu erwarten sei, daß auch Untersuchungsausschüsse diese Rechtsprechung beachteten. Eine Maßnahme der Rechtsaufsicht sei daher entbehrlich. Dies umso begründeter, als der Gesetzgeber wegen der Bedeutung, die er der Unabhängigkeit des BStU beimesse, Maßnahmen der Rechtsaufsicht gegenüber dem BStU der Bundesregierung vorbehalten habe.

In meiner Erwiderung habe ich noch einmal deutlich gemacht, daß meine Empfehlung an die Bundesregierung darauf abzielte, Rechtssicherheit und Rechtsklarheit für die Arbeit künftiger parlamentarischer Untersuchungsausschüsse und für den BStU zu schaffen.

Trotz der Stellungnahme der Bundesregierung halte ich nach wie vor an meiner Position fest, daß eine klare Regelung im Gesetz selbst in diesem empfindlichen Bereich besser wäre. Ich kann aber nicht ausschließen,

daß die Auffassung des BMI in der Praxis die gleiche Wirkung entfaltet und stelle deshalb meine Forderung zunächst zurück. Bei entsprechenden künftigen Fällen werde ich kontrollieren, ob die Rechtsprechung des Landgerichts Kiel beachtet wird. Gegebenenfalls werde ich dann erneut auf eine gesetzliche Regelung drängen.

5.9.2 Weitere Beratungen und Kontrollen des BStU und seiner Außenstellen

Auch im Berichtszeitraum habe ich zwei Außenstellen des BStU beraten und kontrolliert. Erfreulicherweise wird dem Datenschutz beim BStU große Bedeutung zugemessen. Die anläßlich der Besuche festgestellten Mängel wurden nach Möglichkeit umgehend behoben.

In meinem 16. TB (Nr. 5.9.2) habe ich über die Pflicht zur Nachberichtigung nach § 4 Abs. 3 StUG berichtet. Mit Rücksicht auf die Arbeitsbelastung des BStU habe ich mich mit ihm mittlerweile dahingehend verständigt, daß der Wortlaut des § 4 Abs. 3 StUG ihn nicht verpflichtet, alle bereits erteilten Auskünfte mit Hilfe der nun vorhandenen Datei „Elektronisches Personenregister“ daraufhin zu überprüfen, ob die erteilte Auskunft wegen neuer Erkenntnisse berichtigt werden muß. Stellt er jedoch fest, daß sich eine bereits erteilte Auskunft im nachhinein als unrichtig erweist, ist die Auskunft gegenüber dem Empfänger zu berichtigen, sofern die rechtlichen Voraussetzungen weiterhin vorliegen.

Der Sächsische Datenschutzbeauftragte hatte mich auf folgenden Fall aufmerksam gemacht: Ein sächsisches Ministerium hatte im Rahmen der Überprüfung von Mitarbeitern des öffentlichen Dienstes auf eine eventuelle frühere Tätigkeit für das MfS zunächst Auskunft aus den Unterlagen zu einer Angestellten beantragt. Da dem Ministerium die erteilte Auskunft nicht ausreichte, beantragte es Einsicht in die Unterlagen, die daraufhin einem Mitarbeiter des Ministeriums gewährt wurde. Außerdem wurden ihm Kopien der Unterlagen ausgehändigt. Dies alles hätte im Einklang mit den Bestimmungen des Stasi-Unterlagen-Gesetzes stehen können, wenn nicht eine Reihe von Fehlern gemacht worden wäre:

Erstens hätte eine Einsichtnahme gar nicht mehr erfolgen dürfen, denn das Arbeitsverhältnis zwischen dem Ministerium und der Angestellten war mittlerweile durch einen gerichtlichen Vergleich beendet worden. Diese Tatsache war jedoch dem BStU zum Zeitpunkt der Akteneinsicht noch nicht bekannt. Zweitens wurde es seitens des BStU versäumt, in den Unterlagen Angaben über Dritte zu anonymisieren, und drittens wurden auch die an den Mitarbeiter des Ministeriums herausgegebenen Kopien nicht anonymisiert. Nachdem der Sächsische Datenschutzbeauftragte den BStU über die Beendigung des Arbeitsverhältnisses informiert hatte, wurden zwar die nichtanonymisierten Kopien zurückgefordert, aber gleichzeitig der vierte Fehler begangen. Obwohl der BStU nunmehr wußte, daß der Verwendungszweck inzwischen entfallen war, wurden dem Vertreter des Ministeriums die inzwischen anonymisierten Kopien ausgehändigt. Während die erfolgte Einsichtnahme durch den Mitarbeiter des sächsischen Ministeriums trotz zwischenzeitlicher Beendigung des Arbeitsverhältnisses nicht vom BStU zu verantworten war und folglich vom Sächsischen Datenschutzbeauftragten gegenüber dem Ministerium förmlich beanstandet wurde, habe ich das fehlerhafte Handeln des BStU gegenüber dem BMI nach § 25 BDSG beanstandet. In seiner Stellungnahme hat das BMI die beanstandeten Fehler eingeräumt und mitgeteilt, daß der BStU seine Mitarbeiter eindringlich darauf hingewiesen hat, derartige Fehler künftig zu vermeiden.

5.9.3 Benachrichtigung nach § 30 Stasi-Unterlagen-Gesetz

Durch einen Petenten wurde ich darauf aufmerksam gemacht, daß der BStU auf ein Ersuchen nach § 19 i.V.m. § 21 Abs. 1 Nr. 1 StUG Kopien aus seinen Stasi-Unterlagen an ein Landesamt für Rehabilitierung und Wiedergutmachung übermittelt hatte, ohne den Petenten hierüber zu informieren. Der BStU begründete diese bei ihm gängige Praxis damit, daß er davon ausgegangen sei, der Petent sei vom Amt für Rehabilitierung und Wiedergutmachung im Rahmen der Bearbeitung seines Rehabilitierungsverfahrens darüber informiert worden, welche Informationen aus Stasi-Unterlagen an dieses Amt übermittelt würden. Er habe daher darauf verzichtet, den Petenten über die Informationsübermittlung in Kenntnis zu setzen (§ 30 Abs. 2 StUG).

Nach meiner Auffassung ist der BStU jedoch grundsätzlich dazu verpflichtet (§ 30 Abs. 1 StUG), den Betroffenen zu informieren, wenn personenbezogene Unterlagen nach den §§ 21, 27 Abs. 1 und 28 StUG übermittelt werden, wobei diesem die Art der übermittelten Informationen und deren Empfänger mitzuteilen ist. Von dieser Pflicht wird der BStU nach § 30 Abs. 2 StUG u. a. nur dann entbunden, wenn der Betroffene auf andere Weise Kenntnis von der Übermittlung erlangt hat. Dabei ist Voraussetzung, daß dieser **tatsächlich** Kenntnis von der Übermittlung erlangt hat. Allein dessen Möglichkeit, von der Übermittlung auf andere Weise Kenntnis erlangen zu können, reicht für die Befreiung von der Benachrichtigungspflicht nicht aus. Erfreulicherweise hat sich der BStU meiner Rechtsauffassung angeschlossen und mir mitgeteilt, daß er die Benachrichtigung der Betroffenen künftig selbst vornehmen werde.

5.10 Herstellung der Personalausweise und Pässe in der Bundesdruckerei

Die Bundesdruckerei GmbH, deren Anteile zu 100 % der Bundesrepublik Deutschland gehören, und für deren datenschutzrechtliche Beratung und Kontrolle ich daher zuständig bin, hat im Berichtszeitraum für die Herstellung der Personalausweise und Pässe neue Produktionsverfahren und Techniken eingeführt. Auch in der Zusammenarbeit mit den Ausweisbehörden der Kommunen hat sie das Bestell- und Lieferverfahren für die Ausweisdokumente verbessert. Dabei strebt sie insbesondere an, sog. Medienbrüche – also z. B. die Übertragung von Papier auf ein elektronisches Medium und umgekehrt – wegen der damit verbundenen Fehlerquellen weitestgehend zu vermeiden.

Die Bundesdruckerei GmbH räumt, wie meine langjährigen Erfahrungen zeigen, dem Datenschutz einen besonders hohen Stellenwert ein. So hat sie mich bereits frühzeitig über die vorstehenden Planungen informiert, um meine Bewertung zu erhalten. Ich konnte daher bereits zu einer Zeit, zu der Korrekturen in aller Regel noch ohne großen technischen und finanziellen Aufwand möglich sind, Hinweise und Empfehlungen geben.

Zum 1. April 1997 hat die Bundesdruckerei das **Herstellungsverfahren der Personalausweise und Pässe** umgestellt (siehe Abbildung 1).

Während dies für den Bürger nur daran sichtbar wurde, daß sein Ausweis seither ein farbiges Lichtbild enthält, besteht die größte Veränderung darin, daß die von den Kommunen in Papierform übersandten Antragsvordrucke, die vorher die gesamte Produktion parallel begleiteten, nunmehr unmittelbar nach einer Prüfung auf Richtigkeit und Vollständigkeit maschinell gelesen und digitalisiert werden. Alle Daten werden in einer zentralen Datenbank gespeichert und für den jeweiligen Herstellungsschritt dort abgerufen. Auch das Druckverfahren wurde modernisiert, so daß nunmehr bis zu 70 000 Ausweisdokumente pro Tag hergestellt werden können.

Die Bundesdruckerei bietet den Personalausweis- und Paßbehörden auf Wunsch seit kurzem mit dem **– Digitalen Pass- und Ausweis-Sicherheits-System – D-PASS –** einen neuen Service an. Mit D-PASS werden die im Herstellungsprozeß der Ausweisdokumente benötigten digitalen Daten verschlüsselt und anschließend den Ausweisbehörden auf einer CD-Rom zur Verfügung gestellt. Die Bundesdruckerei ist sowohl durch das Personalausweis- als auch durch das Paßgesetz verpflichtet, alle personenbezogenen Ausweisdaten unmittelbar nach der Herstellung der Dokumente zu löschen. Die Einhaltung dieser gesetzlichen Vorgabe wird dadurch erreicht, daß die personenbezogenen Daten kurz vor der gesetzlich vorgeschriebenen Löschung in einer gesonderten Datenbank der Bundesdruckerei in verschlüsselter Form abgelegt werden. Dabei nimmt zwar die Bundesdruckerei die Verschlüsselung selbst vor, aber sie ist nicht in der Lage, diese Daten wieder zu entschlüsseln. Die Daten werden sodann auf eine CD-Rom übertragen, die der bestellenden Ausweisbehörde zugesandt wird; allein diese ist in der Lage, die verschlüsselten Daten zu lesen. Dieses System bietet den Vorteil, daß die Archivierung großer Mengen Papier entfällt und zudem der Zugriff auf die Datenbestände problemlos und ohne größeren Zeitaufwand erfolgen kann.

Ein weiteres neues Projekt der Bundesdruckerei, welches sich derzeit in einer Erprobungsphase befindet, ist das **digitale Antragsverfahren für Reisepässe und Personalausweise – DIGANT –**. Mit diesem Projekt entwickelt die Bundesdruckerei ein Antragsverfahren für Reisepässe und Personalausweise, das den herkömmlichen Papierantrag überflüssig macht und eine durchgängige digitale Erfassung, Verwaltung und Verarbeitung der Antragsdaten ermöglicht. Bei den Personalausweis- und Paßbehörden werden an einem mit einem Scanner ausgestatteten Arbeitsplatz das Paßbild und die Unterschrift bei der Antragstellung digital erfaßt. In einem automatisierten Antragsformular werden alle erforderlichen Daten verschlüsselt und digital signiert über Datenleitungen an die Bundesdruckerei gesendet. Die Verwaltung und Pflege der Paß- und Ausweisregister wird mit DIGANT stark vereinfacht: Archive mit Papierdokumenten entfallen, und für bereits digital geführte Archive beginnt der Weg zum digitalen Archivdatensatz schon bei der Antragstellung.

Aus datenschutzrechtlicher Sicht sehe ich sowohl in dem neuen Herstellungsverfahren als auch in den Verfahren D-PASS und DIGANT eine deutliche Verbesserung der Richtigkeit und Sicherheit der Daten. Sie beruht insbesondere darauf, daß die bislang durch eine manuelle Datenerfassung auftretenden Fehlerquellen deutlich reduziert wurden bzw. werden können.

5.11 Datenübermittlung von Aussiedleraufnahmedaten des BVA an den Suchdienst des Deutschen Roten Kreuzes in Hamburg

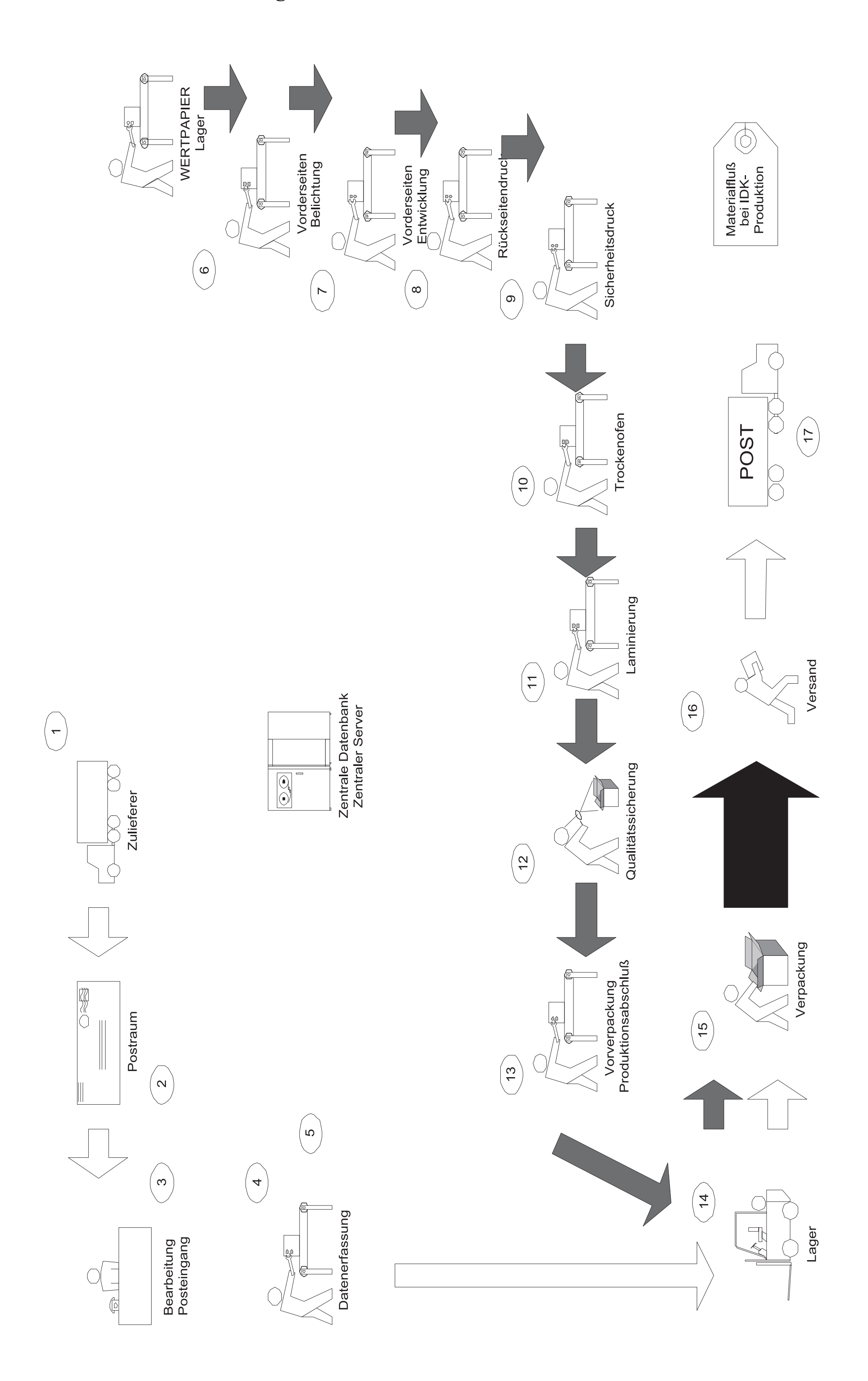
Bereits in meinem 16. TB (Nr. 5.8) habe ich dargestellt, daß der Suchdienst des Deutschen Roten Kreuzes in Hamburg (DRK-Suchdienst) die vom BVA aus dem Aussiedleraufnahmeverfahren übermittelten personenbezogenen Daten derzeit ohne ausreichende Rechtsgrundlage erhält und verarbeitet. Ich habe deshalb dem BMI empfohlen, eine Absichtserklärung dahin abzugeben, daß in absehbarer Zeit eine gesetzliche Regelung für diese Datenübermittlungen auf den Weg gebracht wird. Dieser Empfehlung ist das BMI erfreulicherweise gefolgt.

Mit Schreiben vom 16. Juni 1998 hat das BMI nochmals ausdrücklich auf die Bedeutung der humanitären Aufgaben hingewiesen, die der DRK-Suchdienst im Auftrag der Bundesregierung erfüllt. Zugleich hat das BMI seine Bereitschaft erklärt, den durch das Bundesverfassungsgericht gestellten Anforderungen an die Verarbeitung personenbezogener Daten zu entsprechen und sie für den DRK-Suchdienst sobald wie möglich gesetzlich zu regeln. Ferner sind in diesem Schreiben die Aufgaben, die der DRK-Suchdienst im Auftrag der Bundesregierung im Rahmen der Familienzusammenführung und des Hilfs- und Beratungsdienstes wahrnimmt, im Einzelnen dargelegt und Regelungen zur Datenspeicherung, -nutzung und -sicherheit angesprochen.

Vor dem Hintergrund dieses Schreibens habe ich die Verarbeitung und Nutzung dieser Daten durch den DRK-Suchdienst kontrolliert und dabei einen besonderen Schwerpunkt auf die datenschutzrechtlichen Aspekte bei der Übermittlung von Daten aus dem Aussiedleraufnahmeverfahren vom BVA an den DRK-Suchdienst gelegt.
Der DRK-Suchdienst gliedert sich in die Abteilungen Verwaltung, Familienzusammenführung sowie Hilfs- und Beratungsdienst. Im Bereich der Familienzusammenführung bestehen die Hauptaufgaben in der Unterstützung bei der Lösung humanitärer Probleme. Der DRK-Suchdienst entwickelt dazu Lösungen für eine geordnete Einreise in die Bundesrepublik Deutschland und stützt sich dabei auf seine seit Jahrzehnten aufgebauten Datenbestände. Für diese Arbeit werden ihm personenbezogene Daten aus dem Aussiedleraufnahmeverfahren

Abbildung 1 (zu Nr. 5.10)

Herstellungsverfahren der Personalausweise und Pässe



in einem seiner Aufgabenstellung angepaßten – und damit reduzierten Umfang – durch das BVA übermittelt. Diese Daten sind neben den Angaben aus den Anträgen auf Ausstellung von sog. Wysows (Anforderung des Ausreisewilligen durch einen im Bundesgebiet ansässigen Verwandten*)* und aus freiwillig übersandten Kopien der Aufnahmebescheide die umfassenste Datenquelle des DRK-Suchdienstes. Besonders die BVA-Daten bilden die Grundlage für intensive Nachforschungen in schwierigen Fallkonstellationen. Die Datenbestände des DRK-Suchdienstes werden darüber hinaus aus weiteren Datenquellen ergänzt (z. B. aus Personalbögen des DRK-Suchdienstes, Such- und Sachstandsanfragen von Behörden und Privatpersonen). Mit diesen Daten wird die bereits seit dem Jahr 1951 beim DRK-Suchdienst bestehende Sammlung fortgeführt.

Nach Darstellung des DRK-Suchdienstes wird bei Anfragen und Hilfeersuchen von Aussiedlern zur Familienzusammenführung durch gezielte Computerrecherchen effektive Unterstützung geleistet. Die Daten des BVA dienen aber auch dazu, unvollständige Angaben zu ergänzen, und den Zugang zu dem Betroffenen z. B. über einen bislang dem DRK-Suchdienst unbekannten Bevollmächtigten zu ermöglichen. Auch leisten sie Hilfe in Fällen, in denen Namensänderungen die Suche erschweren. Die Daten werden nach langjährigen Erfahrungen des DRK-Suchdienstes darüber hinaus noch bei weiteren Aufgabenerledigungen benötigt (z. B. Auskunftsbemühungen über die familiäre Situation zum Zeitpunkt der Erteilung des Bescheides durch das BVA, Ermittlung der Einreise oder Identifizierung eines Gesuchten, Staatsangehörigkeitsfeststellungsverfahren des BVA, Suche nach Familienangehörigen).

Im Rahmen meiner Beratung und Kontrolle habe ich mich davon überzeugt, daß der DRK-Suchdienst zur Erfüllung der ihm von der Bundesregierung übertragenen Aufgabenbereiche auf eine Übermittlung ausgewählter Daten aus dem Aussiedleraufnahmeverfahren durch das BVA angewiesen ist. Dies wird voraussichtlich auch in Zukunft so bleiben. Ich gehe davon aus, daß im Rahmen der in Aussicht gestellten gesetzlichen Regelung für die Aufgabenwahrnehmung durch den DRK-Suchdienst die von mir geforderten datenschutzrechtlichen Verbesserungen (z. B. Sicherungsmaßnahmen bei der Datenübermittlung und -speicherung) berücksichtigt werden.

5.12 Ordensangelegenheiten

Im 16. TB (Nr. 5.11) habe ich erstmals ausführlich beschrieben, welche Fragen zum Schutz des Persönlichkeitsrechts sich bei der Erhebung von Daten des für eine Ehrung Vorgeschlagenen im Rahmen der Prüfung der Ordenswürdigkeit stellen können. Die Prüfung der Voraussetzungen für eine Ordensverleihung, d. h. ob die Verdienste des Betroffenen eine Ordensverleihung rechtfertigen und ob der Betroffene einer solchen Auszeichnung würdig erscheint, erfolgt in aller Regel durch die Länder. Die von den vorschlagsberechtigten Stellen (Ministerpräsidenten der Länder und Leiter der obersten Bundesbehörden) mit der Bearbeitung betrauten Arbeitseinheiten stellen üblicherweise Auskunftsersuchen an das BZR und in vielen Fällen an den BStU.

Ich halte es für erforderlich, diese Erhebung von Daten rechtlich zu regeln; denn die Befugnis der vorgenannten Behörden, auf behördliche Anfragen hin Auskünfte zu erteilen, enthält nicht gleichzeitig das Recht zur Erhebung der Daten. Die Feststellung der Bundesregierung in ihrer Stellungnahme zum 16. TB, daß zwischen BMI und BfD Einvernehmen darüber bestehe, die Informationsgewinnung beim BZR und beim BStU sei unproblematisch, ist deshalb unzutreffend. Ich stelle lediglich nicht in Frage, daß Auskünfte aus dem BZR bzw. vom BStU für die Prüfung der Ordenswürdigkeit erforderlich sind.

Den Einwand der Bundesregierung, § 13 Abs. 2 Nr. 2a BDSG reiche als Rechtsgrundlage für das Erheben von Daten ohne Mitwirkung des Betroffenen aus, teile ich nicht. Zum einen umfaßt diese Ausnahmeregelung in erster Linie Aufgaben staatlicher Leistungsgewährung mit oder ohne Antrag des Betroffenen, zum anderen bedeutet *„ohne Mitwirkung“* nicht gleichzeitig *„ohne Kenntnis“*. Der Betroffene muß aber davon in Kenntnis gesetzt werden, daß die vorschlagsberechtigte Stelle in Ordensangelegenheiten beabsichtigt, ihn betreffende – teilweise hochsensible – Daten zu erheben. Ist der Betroffene damit grundsätzlich nicht einverstanden, so muß diese Informationsgewinnung unterbleiben.

In meiner Forderung geht es mir nicht so sehr darum, das Verfahren in bezug auf die Prüfungsreihenfolge der beiden Elemente „Verdienste“ und „Würdigkeit“ gesetzlich zu regeln. Die Bundesregierung hat hier zutreffend geäußert, daß diese Verfahrensänderung auch durch Verwaltungsabsprachen regelbar ist. Dem Betroffenen muß aber – in dem Bewußtsein, daß es bei seiner Nichtzustimmung auf keinen Fall zu einer Ordensverleihung kommen kann – ein Dispositionsrecht eingeräumt werden. Dieses darf nicht deshalb unberücksichtigt bleiben, weil die vorschlagsberechtigte Behörde im Falle einer Ablehnung nach Auffassung des BMI in einen *„unlösbaren Rechtfertigungszwang“* käme.

In der abgelaufenen 13. Legislaturperiode konnte eine entsprechende Rechtsgrundlage für die Erhebung und Verarbeitung personenbezogener Daten im Zusammenhang mit der Vorbereitung der Verleihung eines Verdienstordens der Bundesrepublik Deutschland nicht mehr geschaffen werden. Ich halte aber weiterhin an meiner Empfehlung fest und werde in der neuen Legislaturperiode in Gesprächen mit dem BMI auf eine gesetzliche Grundlage hinwirken.

5.13 Bundeszentrale für politische Bildung

Die Bundeszentrale für politische Bildung (BpB) plant die Einführung eines DV-Verfahrens für die Eingabe von **Be**stellungen, die Verwaltung des **La**gerbestandes und die Erstellung von **Dok**umenten mit dem Namen BELADOK. Die BpB hat mir anläßlich meiner Beratung dieses Verfahren anhand der bereits von der ausführenden Firma vorgelegten Benutzer-Dokumentation erläutert. Dabei mußte ich leider feststellen, daß grundlegende datenschutzrechtliche Anforderungen bei der Planung nicht berücksichtigt worden waren.

Die BpB beabsichtigt, eine Datenbank mit ca. 200 000 Adressen aufzubauen. Das Verfahren sah zunächst vor, daß jeder Mitarbeiter unabhängig von seiner konkreten Aufgabe auf alle Adressen zugreifen und Änderungen vornehmen kann. Hierzu habe ich deutlich gemacht, daß dies im Hinblick auf den datenschutzrechtlichen Grundsatz der Erforderlichkeit problematisch ist, allerdings dann bedenkenfrei sei, wenn die Einwilligung der Betroffenen vorliege. Auch Löschungsfristen für die Adressdaten waren nicht vorgesehen. Hier gilt der Grundsatz, daß Daten nur solange gespeichert werden dürfen, wie es zur Aufgabenerfüllung der speichernden Stelle erforderlich ist. Ein weiteres Problem ist der von der BpB herausgegebene Bestellschein für Publikationen. Darauf befindet sich der Aufdruck, daß die Angaben zu Jahrgang, Geschlecht, Haupt- und Nebenberuf des Bestellers freiwillig sind und nicht personenbezogen sowie ausschließlich im Rahmen der Aufgaben der BpB verarbeitet werden. Die Benutzer-Dokumentation von BELADOK sieht aber eine Trennung dieser für statistische Zwecke erbetenen Daten von den personenbezogenen Adressdaten nicht vor. Der Besteller, der seine Daten also für statistische Zwecke preisgibt, würde getäuscht, denn die BpB könnte jederzeit einen Bezug zwischen den Adressdaten und den freiwilligen Daten herstellen. Ich habe die BpB darauf hingewiesen, daß diese statistischen Daten in das System BELADOK erst dann eingegeben werden dürfen, wenn damit zwangsweise die Trennung von den personenbezogenen Adressdaten verbunden ist.

Erfreulicherweise hat die BpB in ihrer Stellungnahme zugesagt, alle beschriebenen Mängel im Verfahren BELADOK zu beheben. Da sie an dem Konzept einer Gesamtdatenbank mit Zugriff für alle Mitarbeiter festhalten will, soll die Einwilligung der Betroffenen zur Speicherung ihrer Daten eingeholt werden. Ferner wurde zugesichert, bestimmte Adressen nach Ablauf einer festzulegenden Frist automatisch zu löschen und die Trennung der Adressdaten der Besteller der Publikationen von den freiwilligen Daten für statistische Zwecke zu gewährleisten. Das Verfahren BELADOK wird voraussichtlich im Jahre 1999 bei der BpB eingeführt werden.

5.14 Staatsangehörigkeitsdatei im Bundesverwaltungsamt

In meinem 16. TB (Nr. 5.7) berichtete ich ausführlich über die beim Bundesverwaltungsamt geführte Staatsangehörigkeitsdatei. Da eine Rechtsgrundlage für diese Datei fehlt, habe ich mich mit dem BMI bis zur Entscheidung des Gesetzgebers auf bestimmte Feststellungen und Verfahrensweisen geeinigt. Trotz umfassender Diskussionen ist es bis zum Ende der vergangenen Legislaturperiode nicht zu einer Neuregelung des deutschen Staatsangehörigkeitsrechts gekommen. Auch die hilfsweise angestrebte Lösung, die Staatsangehörigkeitsdatei in Verbindung mit einem anderen Gesetz auf eine rechtliche Grundlage zu stellen, konnte nicht verwirklicht werden. Ich werde daher weiterhin darauf drängen, das Führen der Staatsangehörigkeitsdatei alsbald gesetzlich zu regeln.

6 Rechtswesen

6.1 Akustische Wohnraumüberwachung

Die Diskussion um die Änderung von Artikel 13 GG (Unverletzlichkeit der Wohnung) wegen der Einführung der akustischen Wohnraumüberwachung für Strafverfolgungszwecke nahm in der vergangenen Legislaturperiode im Bereich der inneren Sicherheit eine herausragende Stellung ein. An dieser Diskussion, die unter dem Stichwort „Großer Lauschangriff“ auch in den Medien große Beachtung fand, haben sich nahezu alle gesellschaftspolitischen Kräfte in der Bundesrepublik Deutschland beteiligt. Ein derart breites Forum halte ich bei einer Thematik, die den Schutz der Privatsphäre der Menschen in ihrem engsten Bereich betrifft, für ein außerordentlich positives Zeichen. Ich selbst habe die Beratungen der verschiedenen Gesetzentwürfe intensiv begleitet und meine Empfehlungen sowohl bei der Bundesregierung als auch in den zuständigen parlamentarischen Gremien eingebracht. Bereits in meinem 16. TB (Nr. 6.1.1) bin ich ausführlich auf dieses Thema eingegangen; die seinerzeit gegebenen Empfehlungen sind in den verabschiedeten Gesetzen weitgehend berücksichtigt worden.

6.1.1 Gesetz zur Änderung des Grundgesetzes (Artikel 13)

Das Gesetz zur Änderung des Grundgesetzes (Artikel 13) vom 26. März 1998 (BGBl. I S. 610) regelt – entgegen einer oft verbreiteten Darstellung – nicht die allgemeine Einführung der akustischen Wohnraumüberwachung. Vielmehr sehen die Polizeigesetze der meisten Bundesländer die Möglichkeit einer Erhebung personenbezogener Daten zur **Gefahrenabwehr** in bzw. aus Wohnungen durch den Einsatz technischer Mittel schon lange vor. Der Gesetzgeber hat für diesen Bereich durch die Grundgesetzänderung einheitliche Vorgaben geschaffen, zusätzliche verfassungsrechtliche Schranken gezogen und damit zu einer Anhebung des Schutzniveaus in den Polizeigesetzen beigetragen. Darüber hinaus wird jetzt durch die Änderung des Artikel 13 GG auch der Einsatz technischer Mittel zum Abhören und Aufzeichnen des gesprochenen Wortes in Wohnungen für Zwecke der **Strafverfolgung** zugelassen.

Mit dieser Änderung wurde Artikel 13 um die Absätze 3 bis 6 erweitert; sie sehen folgende Regelungen vor:

– Nach Artikel 13 **Abs. 3** GG darf der Einsatz technischer Mittel zur akustischen Überwachung von Wohnungen, in denen sich der Beschuldigte vermutlich aufhält, für **Zwecke der Strafverfolgung** richterlich angeordnet werden, wenn bestimmte Tatsachen den Verdacht begründen, daß jemand eine durch Gesetz einzeln bestimmte besonders schwere Straftat begangen hat und die Erforschung des Sachverhalts auf andere Weise unverhältnismäßig erschwert oder aussichtslos wäre. Diese Maßnahme muß zeitlich befristet werden und wird durch einen mit drei Richtern besetzten Spruchkörper angeordnet; bei Gefahr in Verzug kann sie auch durch den Einzelrichter getroffen werden. Gegenstand der Überwachung sind nur

die Wohnungen, in denen sich der Beschuldigte vermutlich aufhält. Andere technische Mittel, wie z. B. die Videoüberwachung, sind unzulässig.

– Nach Artikel 13 **Abs. 4** GG dürfen zur **Abwehr dringender Gefahren** für die öffentliche Sicherheit technische Mittel zur Überwachung von Wohnungen nur aufgrund richterlicher Anordnung eingesetzt werden. Zulässig sind damit – wie auch schon vor der Änderung des Grundgesetzes – sowohl akustische als auch optische Überwachungsmaßnahmen. Bei Gefahr in Verzug kann die Maßnahme auch durch eine andere gesetzlich bestimmte Stelle angeordnet werden; eine richterliche Entscheidung ist unverzüglich nachzuholen.

– Sind technische Mittel ausschließlich zum **Schutze der bei einem Einsatz in Wohnungen tätigen Personen** vorgesehen, kann die Maßnahme durch eine gesetzlich bestimmte Stelle angeordnet werden (Artikel 13 **Abs. 5** GG). Eine anderweitige Verwertung der hierbei erlangten Erkenntnisse ist nur zum Zwecke der Strafverfolgung oder der Gefahrenabwehr und nur dann zulässig, wenn zuvor die Rechtmäßigkeit der Maßnahme richterlich festgestellt ist; bei Gefahr im Verzuge ist die richterliche Entscheidung unverzüglich nachzuholen. Die Maßnahme muß also ausschließlich der sog. **Eigensicherung** gedient haben und darf auch nicht teilweise das Ziel verfolgt haben, darüber hinausgehende Informationen zu gewinnen.

– Gemäß Artikel 13 **Abs. 6** GG wird die Bundesregierung verpflichtet, den **Bundestag jährlich** über die akustischen Wohnraumüberwachungen zu **unterrichten**, die für Zwecke der Strafverfolgung durchgeführt wurden. Dies gilt auch für den Einsatz technischer Mittel nach Absatz 4, soweit dieser im Zuständigkeitsbereich des Bundes erfolgte, und nach Absatz 5, soweit eine richterliche Überprüfungsbedürftigkeit bestand. Ein vom Bundestag gewähltes Gremium übt auf der Grundlage dieses Berichts die parlamentarische Kontrolle aus. Die Länder gewährleisten eine gleichwertige parlamentarische Kontrolle.

Die Änderungen von Artikel 13 GG entsprechen im wesentlichen meinen Empfehlungen. Unabdingbar war und ist für mich, daß für Zwecke der Strafverfolgung nur dann in das Grundrecht eingegriffen werden darf, wenn besonders schwere Straftaten begangen wurden, die im Gesetz im einzelnen zu bestimmen sind. Die verfassungsrechtliche Verankerung von Verfahrensgrundsätzen für die Wohnraumüberwachung zur Gefahrenabwehr und zur Eigensicherung nicht offen ermittelnder Personen begrüße ich als Klarstellung ebenfalls.

Bedenken habe ich dagegen, auch optische Mittel bei der Wohnraumüberwachung einzusetzen. Da dies aber für Zwecke der Gefahrenabwehr weiterhin möglich ist, sollte bundesweit vorgesehen werden, die Aufzeichnungen unmittelbar nach dem Einsatz zu löschen. Ansonsten könnten nämlich diese Aufzeichnungen auch für die Verfolgung von Straftaten verwendet werden und damit würde genau das eintreten, was zu repressiven Zwecken gerade nicht gewollt ist.

Besonders positiv hervorzuheben sind die umfangreichen Berichtspflichten an das Parlament. Diese wurden erfreulicherweise noch ergänzt durch einen Beschluß des Deutschen Bundestages, demzufolge die Bundesregierung unabhängig von der Berichtspflicht nach Artikel 13 Abs. 6 GG spätestens zum 31. Januar 2002 einen detaillierten Erfahrungsbericht zu den Wirkungen der Wohnungsüberwachung durch Einsatz technischer Mittel vorzulegen hat, der eine Bewertung der Gesetzesfolgen mit verfassungsrechtlicher und kriminalpolitischer Würdigung der bis dahin durchgeführten Maßnahmen der Überwachung einschließt.

6.1.2 Gesetz zur Verbesserung der Bekämpfung der Organisierten Kriminalität

Mit dem Gesetz zur Verbesserung der Bekämpfung der Organisierten Kriminalität vom 4. Mai 1998 (BGBl. I S. 845) hat der Gesetzgeber das rechtliche Instrumentarium zur Bekämpfung der Organisierten Kriminalität durch Ergänzungen des Strafgesetzbuches, der Strafprozeßordnung, des Geldwäschegesetzes und des Finanzverwaltungsgesetzes erweitert. Im Bereich der Strafprozeßordnung ist das strafprozessuale Ermittlungsinstrumentarium der Strafverfolgungsbehörden um die akustische Überwachung von Wohnräumen ergänzt worden. Die Wohnraumüberwachung soll auch dazu beitragen, in Kernbereiche von kriminellen Organisationen einzudringen und deren Strukturen aufzuhellen. Bei diesen Vorschriften handelt es sich um die einfachgesetzliche Ausprägung der Änderung des Artikel 13 GG (s. o. Nr. 6.1.1).

Gemäß § 100c Abs. 1 Nr. 3 StPO darf das in einer Wohnung nichtöffentlich gesprochene Wort des Beschuldigten mit technischen Mitteln abgehört und aufgezeichnet werden, wenn bestimmte Tatsachen den Verdacht begründen, daß er eine der in § 100c Abs. 1 Nr. 3 lit a bis f StPO genannten Katalogtaten begangen hat und die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Täters auf andere Weise unverhältnismäßig erschwert oder aussichtslos wäre. Diese Maßnahmen dürfen grundsätzlich nur in Wohnungen des Beschuldigten durchgeführt werden; in Wohnungen anderer Personen sind sie nur zulässig, wenn aufgrund bestimmter Tatsachen anzunehmen ist, daß der Beschuldigte sich in diesen Wohnungen aufhält (§ 100c Abs. 2 Satz 4 und 5 StPO).

In der Diskussion um die Ausgestaltung der akustischen Wohnraumüberwachung war für mich der Schutz des Vertrauensverhältnisses der Bürger zu Angehörigen bestimmter Berufsgruppen wie Ärzte, Rechtsanwälte, Geistliche, Abgeordnete und Journalisten ein ganz entscheidender Punkt. Das geltende **Zeugnisverweigerungsrecht** dieser Personen und ihrer Berufshelfer dient primär nicht ihrer ungestörten Berufsausübung, sondern in erster Linie den Patienten, Klienten, Informanten etc., die sich hilfe- und vertrauensuchend an diese Personen wenden. Deshalb habe ich gefordert, daß Räume, in denen diese Personen üblicherweise ihren Beruf ausüben, wie z. B. die Arztpraxis, – und damit zusammenhängend auch ihre Telekommunikationsverbindungen –

von der Überwachung für Strafverfolgungszwecke ausgenommen werden. Dabei geht es mir nicht um eine Ausweitung von Persönlichkeitsrechten zu Lasten der Durchsetzung des staatlichen Strafanspruchs, sondern um den Erhalt herkömmlicher Wertentscheidungen auch im Zeitalter moderner Ermittlungstechnik. Nach langen Erörterungen und der Einschaltung des Vermittlungsausschusses ist zu Gunsten **aller zeugnisverweigerungsberechtigten Personen ein Beweiserhebungsverbot gesetzlich** festgelegt worden; eine Ausnahme gilt berechtigterweise dann, wenn dieser Personenkreis selbst tatverdächtig ist (§ 100d Abs. 3 StPO).

Die Wohnraumüberwachung ist auch unzulässig, wenn zu erwarten ist, daß sämtliche aus der Maßnahme zu gewinnenden Erkenntnisse einem **Verwertungsverbot** unterliegen. In solchen Fällen verbietet bereits der Verhältnismäßigkeitsgrundsatz die Anwendung von Maßnahmen, die nur zur Gewinnung unverwertbarer Erkenntnisse führen können, da sie nicht geeignet sind, das strafverfahrensrechtliche Ziel zu erreichen.

Den im Ergebnis erreichten Schutz der Berufsgeheimnisträger begrüße ich sehr, da der Gesetzgeber zum einen den geschützten Personenkreis weit gefaßt hat und zum anderen der Schutz in jeder Wohnung gilt, also nicht auf die der Berufstätigkeit dienenden Räume beschränkt ist.

Eine Anordnung zur akustischen Wohnraumüberwachung ist auf höchstens vier Wochen zu befristen; eine Verlängerung ist möglich, sofern die Voraussetzungen fortbestehen (§ 100d Abs. 4 StPO). Die Anordnungsbefugnis liegt bei bestimmten Strafkammern des Landgerichts, bei Gefahr im Verzug kann der Vorsitzende allein die Anordnung treffen; dessen Anordnung tritt außer Kraft, wenn sie nicht binnen drei Tagen von der Strafkammer bestätigt wird (§ 100d Abs. 2 StPO). Leider hat der Gesetzgeber nicht die Frage beantwortet, was für die gewonnenen Erkenntnisse gelten soll, wenn die Bestätigung ausbleibt oder abgelehnt wird. Aus meiner Sicht ist in solchen Fällen von einem Verwertungsverbot auszugehen. Liegen die für eine Wohnraumüberwachung erforderlichen Voraussetzungen nicht mehr vor, so sind die sich aus der Anordnung ergebenden Maßnahmen unverzüglich zu beenden; die erlangten Unterlagen sind unverzüglich zu vernichten, wenn sie zur Strafverfolgung nicht mehr erforderlich sind (§ 100d Abs. 4 Satz 3 StPO).

Die Verwendung von personenbezogenen Informationen, die durch eine Wohnraumüberwachung ermittelt worden sind, dürfen unter bestimmten Voraussetzungen sowohl **in anderen Strafverfahren zu Beweiszwecken** (§ 100d Abs. 5 Satz 2 StPO) **als auch zur Gefahrenabwehr** (§ 100f Abs. 1 StPO) verwendet werden. Auch die durch eine polizeirechtliche Maßnahme erlangten Informationen dürfen unter bestimmten Voraussetzungen zu Beweiszwecken verwendet werden (§ 100f Abs. 2 StPO). In den parlamentarischen Beratungen habe ich vergeblich zu erreichen versucht, die Worte *„zu Beweiszwecken“* zu streichen, um die Zweckbindung der erlauschten Informationen zu verdeutlichen. Gespächsinhalte, die mit den verfolgten Verbrechen nichts zu tun haben, sollten nicht als sog. Ermittlungsansatz zur Verfolgung von Bagatell- und Kleinkriminalität verwandt werden dürfen; ansonsten sehe ich die Gefahr einer Umgehung des grundgesetzlich gebotenen Straftatenkataloges.

Die **Beteiligten einer Überwachungsmaßnahme sind zu benachrichtigen**, sobald dies ohne Gefährdung des Untersuchungszweckes möglich ist, was ihnen die Möglichkeit einräumt, ihrerseits die Rechtmäßigkeit der Abhörmaßnahme durch ein Gericht überprüfen zu lassen (§§ 101 Abs. 1, 100d Abs. 6 StPO). Die **Berichtspflichten** gegenüber der obersten Justizbehörde bzw. dem Deutschen Bundestag sind in § 100e StPO geregelt (siehe auch Nr. 11.2).

Im Ergebnis halte ich die Regelungen zur akustischen Wohnraumüberwachung für einen tragfähigen Kompromiß zwischen einem aus Expertensicht wichtigen Mittel zur Bekämpfung der Organisierten Kriminalität und dem Schutz der Privatsphäre des Menschen. Die vorgesehenen Schutzvorkehrungen, die einen Mißbrauch der akustischen Wohnraumüberwachung verhindern sollen, halte ich für ausreichend. Besondere Bedeutung messe ich dem Erfahrungsbericht der Bundesregierung zu (s. o. Nr. 6.1.1), von dem ich mir Aufschluß über die kriminalistische wie auch datenschutzrechtliche Tragweite der Maßnahmen erwarte.

6.2 Entwurf des Strafverfahrensänderungsgesetzes 1996 – StVÄG 1996 –

In den vergangenen Tätigkeitsberichten habe ich mehrfach über die Notwendigkeit einer Novellierung der StPO berichtet (zuletzt 16. TB Nr. 6.1.2). Obgleich inzwischen seit dem Volkszählungsurteil des Bundesverfassungsgerichts vom 15. Dezember 1983 mehr als fünfzehn Jahre vergangen sind, werden ausgerechnet im Bereich der Justiz besonders schützenswerte personenbezogene Daten nach wie vor ohne die von dem Gericht geforderten bereichsspezifischen gesetzlichen Grundlagen erhoben und verarbeitet. Ich halte diesen Zustand für kaum noch vertretbar und befürchte, daß eine Berufung auf den sog. **Übergangsbonus** des BVerfG nicht mehr länger möglich sein wird. Der Entwurf des StVÄG 1996, mit dem die Lücken des Persönlichkeitsschutzes im Strafverfahren geschlossen werden sollten, konnte in der abgelaufenen Legislaturperiode nicht abschließend beraten werden.

Bereits der Regierungsentwurf des StVÄG 1996 war in Teilbereichen den Vorgaben des BVerfG nicht gerecht geworden und teilweise hinter den bereits erreichten Standard der allgemeinen Datenschutzgesetze und anderer bereichspezifischer Regelungen, wie z. B. dem BZRG und den Polizeigesetzen der Länder, zurückgefallen. Insbesondere folgende Punkte habe ich kritisiert:

- Die Voraussetzungen für Maßnahmen der Öffentlichkeitsfahndung sind nicht hinreichend bestimmt, insbesondere muß hier zwischen Beschuldigten und Zeugen angemessen differenziert werden.
- Für Privatpersonen und Stellen, die nicht Verfahrensbeteiligte sind, wird als Voraussetzung zur Auskunfts- und Akteneinsicht lediglich ein vages *„berechtigtes“* statt eines *„rechtlichen“* Interesses gefordert.

– Die Regelungen über Inhalt, Ausmaß und Umfang von Dateien und Informationssystemen mit personenbezogenen Daten bei den Staatsanwaltschaften sind unzureichend, Zugriffsmöglichkeiten der Strafverfolgungs- und Strafjustizbehörden sind zu weitgehend und Standardmaßnahmen des technischen und organisatorischen Datenschutzes (z. B. Protokollierung, interne Zugriffsbeschränkungen) werden abgeschwächt.

Die zu diesem Gesetzentwurf vom Bundesrat am 21. Februar 1997 abgegebene Stellungnahme enthielt im wesentlichen datenschutzrechtliche Verschlechterungen, die vor allem die Entfernung mehrerer im Gesetzentwurf noch vorhandener Beschränkungen und verfahrensrechtlicher Sicherungen zum Schutz des Persönlichkeitsrechts und des Rechts auf informationelle Selbstbestimmung des Betroffenen zum Inhalt haben. Beabsichtigt war beispielhaft:

– Der Richtervorbehalt für die Anordnung der Öffentlichkeitsfahndung und der längerfristigen Observation sollte gestrichen werden.
– Die Verwendungsbeschränkungen bei Daten, die mit besonderen Erhebungsmethoden nach dem Polizeirecht gewonnen wurden, sollten herausgenommen werden.
– Detaillierte Regelungen für die Übermittlung von personenbezogenen Daten von Amts wegen durch Strafverfolgungs- und Strafjustizbehörden an andere Stellen sollten gestrichen werden.
– Speicherungs- und Löschungsfristen für personenbezogene Daten in Dateien sollten ersatzlos gestrichen werden.

Die Datenschutzbeauftragten des Bundes und der Länder haben sich im Rahmen ihrer 53. Konferenz mit dem Entwurf des StVÄG 1996 befaßt und Empfehlungen formuliert (s. Entschließung vom 17./18. April 1997, **Anlage 7**).

Der Rechtsausschuß des Deutschen Bundestages hat sich in zahlreichen Sitzungen der Berichterstatter bemüht, auf der Grundlage des StVÄG 1996 einen mit den Bundesländern abgestimmten Gesetzentwurf noch vor Ablauf der Legislaturperiode einzubringen. In diese intensiven Beratungen bin ich miteinbezogen worden und habe meine Forderungen darlegen können. Verschiedenen Kompromissen habe ich seinerzeit zugestimmt, da ich die Verabschiedung eines Gesetzes, das nicht in allen Punkten meinen Vorstellungen entsprochen hätte, im Vergleich zu dem Zustand einer nicht vorhandenen Rechtsgrundlage vorgezogen habe; im Wege einer Gesetzesnovellierung hätten sich datenschutzrechtliche Mängel in dieser Legislaturperiode beheben lassen können.

Ich halte es für dringend notwendig, wegen der mit der Datenerhebung, Verarbeitung und Nutzung verbundenen Rechtseingriffe in der neuen Legislaturperiode unverzüglich bereichsspezifische Regelungen zu schaffen. In diesem Sinne haben sich auch die Datenschutzbeauftragten des Bundes und der Länder bei ihrer 56. Konferenz geäußert (s. Entschließung vom 5./6. Oktober 1998, **Anlage 15**). Gegenüber dem BMJ habe ich nachdrücklich betont, daß dieses Gesetzgebungsvorhaben oberste Priorität genießen muß und weitere Verzögerungen nicht hinnehmbar sind.

6.3 Genomanalyse im Strafverfahren

Über gesetzgeberische Absichten, Regelungen für den Einsatz gentechnischer Methoden im Strafverfahren zu schaffen, habe ich bereits ausführlich berichtet (16. TB Nr. 6.2). Ich habe gefordert, daß hier gesetzliche Regelungen unerläßlich sind. Denn daß die Genomanalyse tief in das allgemeine Persönlichkeitsrecht des Betroffenen eingreifen kann, machen Berichte um den wissenschaftlichen Fortschritt der Gentechnologie immer wieder deutlich.

Mit dem Strafverfahrensänderungsgesetz – DNA-Analyse – vom 17. März 1997 (BGBl. I S. 534) ist der Gesetzgeber diesen Empfehlungen gefolgt und hat die Voraussetzungen sowie Begrenzungen festgelegt, die für die strafprozessuale Nutzung der DNA-Analyse, des sog. genetischen Fingerabdrucks, im anhängigen Strafverfahren gelten. Die neue Vorschrift des § 81e StPO erlaubt molekulargenetische Untersuchungen an Blutproben oder Körperzellen, die dem Beschuldigten entnommen worden sind, und an entsprechendem Spurenmaterial nur insoweit, als die Untersuchungen zur Feststellung der Abstammung oder der Tatsache erforderlich sind, ob aufgefundenes Spurenmaterial von dem Beschuldigten, dem Verletzten oder einem Dritten stammt. Diese Untersuchungen können deshalb immer nur mit einem eindeutigen Ergebnis abgeschlossen werden, nämlich ob eine Übereinstimmung vorliegt oder nicht. Ausdrücklich wird untersagt, im Strafverfahren angefallenes DNA-analysefähiges Material auf psychische, charakter- oder krankheitsbezogene Persönlichkeitsmerkmale oder Erbanlagen hin zu untersuchen. Die Zulässigkeit einer DNA-Analyse ist nicht an eine besondere Eingriffsschwelle gebunden, so daß ein Beschuldigter bereits bei Vorliegen eines Anfangsverdachts durch eine molekulargenetische Untersuchung belastet, aber auch entlastet werden kann. Die gesetzliche Regelung enthält ferner Verfahrensvorschriften, die die Anordnung und Durchführung der Untersuchung betreffen, wie z. B. den Anordnungsvorbehalt des Richters in § 81f StPO. Die dem Beschuldigten entnommenen Blutproben oder sonstigen Körperzellen dürfen zum Zwecke der Strafverfolgung nur in dem Strafverfahren, für das die Entnahme erfolgte, oder in einem anderen anhängigen Strafverfahren verwendet werden. Sobald sie hierfür nicht mehr erforderlich sind, müssen sie unverzüglich vernichtet werden. Diese Zweckbindungs- und Vernichtungsvorschrift betrifft jedoch nur das für die Untersuchung verwendete Material, nicht jedoch deren Ergebnisse; diese werden als verfahrensrelevante Unterlagen zum Bestandteil der Strafverfahrensakte. Eine Festlegung, ob und in welchen Grenzen eine Speicherung der durch eine DNA-Analyse gewonnenen Untersuchungsergebnisse in Datenbanken für erkennungsdienstliche Zwecke zulässig ist, enthält dieses Gesetz jedoch nicht.

Dieser Thematik haben sich die Datenschutzbeauftragten des Bundes und der Länder im Rahmen ihrer 53. Kon-

ferenz angenommen und ergänzend zu den §§ 81e und f StPO für die automatisierte Speicherung und Nutzung von DNA-Identitätsdaten eine spezielle gesetzliche Regelung in der StPO gefordert, um das Persönlichkeitsrecht des Betroffenen zu schützen (s. Entschließung vom 17./18. April 1997, **Anlage 8**).

Anfang 1998 kündigte das BMJ die Einrichtung einer zentralen Gen-Datenbank zur Überführung insbesondere von Sexual- und Gewaltverbrechern und die Schaffung einer gesetzlichen Grundlage hierfür an. Die öffentliche Diskussion über das Für und Wider einer solchen Datenbank führte – beeinflußt auch durch mehrere schwere Sexualstraftaten an Kindern, die bundesweit für Aufsehen sorgten – schnell dazu, daß sich alle maßgebenden Kräfte zwar über das Ziel der Einrichtung einer Gen-Datenbank verständigten, nicht jedoch über den Weg. Ich habe in dieser Diskussion nachdrücklich die Schaffung einer normenklaren gesetzlichen Regelung mit wichtigen Kriterien für eine Speicherung gefordert. Solche Kriterien sind für mich

- die Prognose, daß ein Beschuldigter mit hoher Wahrscheinlichkeit für künftige Straftaten als Täter in Frage kommt, und
- die Voraussicht, daß die Speicherung seiner DNA-Daten geeignet sein kann, ihn als Straftäter der prognostizierten Art zu erkennen.

Großen Wert habe ich darauf gelegt, daß der in einem aktuellen Strafverfahren gewonnene genetische Fingerabdruck nicht automatisch in die Gen-Datenbank übernommen wird, sondern nur nach einer einzelfallbezogenen Abwägung.

Dieser Empfehlung ist die Bundesregierung zunächst nur zum Teil gefolgt. So hat das BKA mit Zustimmung des BMI im April 1998 bereits eine Errichtungsanordnung (hierzu siehe auch **Anlage 6**) für eine zentrale DNA-Analyse-Datei erlassen, die die Speicherung der gemäß §§ 81e und f StPO angefallenen genetischen Fingerabdrucke auf der Grundlage des § 8 Abs. 6 BKAG für zulässig ansieht. Hier sah ich als problematisch an, daß diese Vorschrift wohl lediglich die Speicherung solcher Daten rechtfertigt, die bei der Durchführung erkennungsdienstlicher Maßnahmen erhoben worden sind; die molekulargenetische Untersuchung gemäß § 81e StPO stellt jedoch keine „erkennungsdienstliche Maßnahme“ im Sinne des § 8 Abs. 6 BKAG dar. Mir wurde jedoch eine Erweiterung der StPO signalisiert, um die DNA-Analyse-Datei, so wie politisch gewollt, aufbauen zu können.

Ansonsten entspricht diese Errichtungsanordnung im wesentlichen meinen Anforderungen. Wichtig ist dabei, daß die gespeicherten Daten zu löschen sind, wenn ihre Speicherung unzulässig oder nicht mehr erforderlich ist. Unzulässig ist eine Speicherung, wenn der Tatverdacht gegen den Beschuldigten ausgeräumt oder er rechtskräftig freigesprochen wurde. Mit der Speicherung der ersten Datensätze wurde am 17. April 1998 begonnen. Bei Redaktionsschluß waren insgesamt 779 Datensätze, davon 509 Spurendatensätze aus Verfahren mit noch nicht ermittelten Verdächtigten, gespeichert.

Mit dem Gesetz zur Änderung der Strafprozeßordnung (DNA-Identitätsfeststellungsgesetz) vom 7. September 1998 (BGBl. I S. 2646) wurde dann die StPO noch einmal erweitert. In Ergänzung zur bisherigen Rechtslage dürfen nach der neu eingefügten Vorschrift des § 81g StPO zum Zwecke der Identitätsfeststellung in künftigen Strafverfahren molekulargenetische Untersuchungen bei Beschuldigten durchgeführt werden, die einer Straftat von erheblicher Bedeutung verdächtig sind. Der Begriff der *„Straftat von erheblicher Bedeutung“* wird durch eine Aufzählung mehrerer schwerer Verbrechen konkretisiert. Zusätzlich muß jedoch Grund zu der Annahme bestehen, daß gegen die Beschuldigten künftig erneut Strafverfahren wegen einer einschlägigen Straftat zu führen sind. Unter den gleichen Voraussetzungen dürfen solche Maßnahmen auch bei bereits rechtskräftig Verurteilten durchgeführt werden (§ 2 DNA-Identitätsfeststellungsgesetz). Die Speicherung dieser vorgenannten Daten richtet sich nach dem BKA-Gesetz; Auskünfte dürfen nur für Zwecke eines Strafverfahrens, der Gefahrenabwehr und der internationalen Rechtshilfe hierfür erteilt werden (§ 3 DNA-Identitätsfeststellungsgesetz).

Diese neuen Regelungen entsprechen weitgehend meinen Empfehlungen. Kritisch ist lediglich anzumerken, daß durch das DNA-Identitätsfeststellungsgesetz keine gesetzliche Grundlage für die Speicherung der Daten geschaffen wurde, die aufgrund § 81e StPO bis zum Inkrafttreten des genannten Gesetzes erhoben wurden. Meine Forderung nach einer Prognose, daß der Beschuldigte und der bereits rechtskräftig Verurteilte auch künftig Straftaten, die in § 81 g StPO bezeichnet sind, begehen werden, ist berücksichtigt. Mit der Möglichkeit der Nachuntersuchung bei den Altfällen, in denen die Strafe bereits verbüßt ist, sollte sensibel umgegangen werden. Hier wird an die Prognose bei jemanden, der wegen einer nicht sexuell bedingten Straftat verurteilt worden war, sicher eine andere Anforderung zu stellen sein als bei Sexualstraftätern. Positiv hervorzuheben ist ferner, daß sowohl die Anordnung der Untersuchung als auch die Prognose selbst dem Richtervorbehalt unterliegen.

Im Ergebnis wahren die neuen Bestimmungen den Anspruch der Allgemeinheit auf innere Sicherheit und respektieren das Persönlichkeitsrecht des Betroffenen. Hinsichtlich der schnellen Fortschritte der DNA-Analyse ist auch künftig sicherzustellen, daß nur die zu Identifizierungszwecken benötigten, die sog. nicht codierenden, Erbinformationen erhoben, gespeichert und verwendet werden und die Gewinnung, Speicherung oder gar Übermittlung von „Überschußinformationen“ ausgeschlossen ist. Die Entwicklung, vor allen Dingen aber auch die Effektivität und Nutzung der DNA-Analyse-Datei werde ich in den nächsten Jahren aufmerksam verfolgen.

6.4 Zugriff der Strafverfolgungsbehörden auf Telekommunikationsdaten – Neufassung des § 12 FAG?

Durch das Telekommunikationsgesetz (TKG) aus dem Jahre 1996 wurde § 12 Fernmeldeanlagengesetz (FAG), dessen zeitliche Geltungsdauer bereits früher bis zum

31. Dezember 1997 befristet worden war, inhaltlich neu gefaßt. Nach dieser Vorschrift kann in strafgerichtlichen Verfahren der Richter Auskunft von Telekommunikationsunternehmen darüber verlangen, wer wann wie lange mit wem kommuniziert hat; es geht dabei also nicht um die Überwachung der Gesprächsinhalte. Auch im Hinblick auf die zeitliche Befristung des § 12 FAG schlug die Bundesregierung im Entwurf des Begleitgesetzes zum TKG als Nachfolgeregelung einen neuen § 99a StPO vor. Hierin sollten die Voraussetzungen, unter denen Auskünfte über die näheren Umstände der Telekommunikation der Betroffenen verlangt werden können, und der Kreis der zur Auskunft Verpflichteten präzisiert werden. So war einerseits vorgesehen, bei solchen Straftaten, die unter Benutzung von Telefonapparaten begangen werden, d. h. beispielsweise Straftaten im Zusammenhang mit beleidigenden und belästigenden Telefonanrufen, alles unverändert zu lassen, während andererseits durch eine Beschränkung des Auskunftsersuchens auf „Straftaten von nicht unerheblicher Bedeutung“ eine Ausweitung des Anwendungsbereichs im übrigen vermieden werden sollte.

Generell habe ich die Absicht begrüßt, § 12 FAG durch eine Neufassung zu ersetzen, die der Entwicklung der modernen Telekommunikation und der damit verbundenen besonderen Nachhaltigkeit staatlicher Eingriffsbefugnisse in diesem Bereich Rechnung trägt. Sowohl im Vorfeld als auch in den parlamentarischen Beratungen habe ich aber kritisiert, daß dieser Entwurf keine Schutzklausel für Telefonate von Personen, die zur Wahrung von Berufsgeheimnissen verpflichtet sind, enthält. Dadurch wird der vom Gesetzgeber durch die Zeugnisverweigerungsrechte gemäß §§ 53 und 53a StPO anerkannte Schutz des Vertrauensverhältnisses zwischen bestimmten Berufsangehörigen und Dritten, die deren Hilfe und Sachkunde in Anspruch nehmen, in diesem Anwendungsbereich unterlaufen. Dabei geht es nicht darum, zugunsten einer Erweiterung von Persönlichkeitsrechten einen Anspruch auf Wahrheitsfindung zu beschränken, sondern eine vom Gesetzgeber bereits gezogene Grenzlinie auch bei geänderten tatsächlichen Bedingungen und Möglichkeiten der modernen Telekommunikation beizubehalten.

Auch die geplante Eingrenzung der Auskunftsersuchen durch den Begriff einer „Straftat von nicht unerheblicher Bedeutung“ sehe ich als wenig geeignet an, dem Gebot der Normenklarheit zu genügen; der Gesetzgeber sollte hier möglichst präzise normative Vorgaben machen.

Darüber hinaus fehlte im Entwurf eine Regelung über die Vernichtung der für die Strafverfolgung nicht bzw. nicht länger erforderlichen Daten. Eine am Grundsatz der Verhältnismäßigkeit orientierte Informationsgewinnung im Strafverfahren erfordert die Vernichtung der nicht mehr benötigten personenbezogenen Daten, so daß ich eine am Regelungsgehalt des § 100b Abs. 6 StPO ausgerichtete Vorschrift empfohlen habe. Schließlich habe ich auch vorgeschlagen, den Entwurf um eine Regelung zu ergänzen, die eine Benachrichtigung der von der Maßnahme betroffenen Person zum Inhalt hat.

In den Beratungen der Ausschüsse des Deutschen Bundestages hat sich erfreulicherweise die Auffassung durchgesetzt, daß der Entwurf der Bundesregierung keine sachgerechte Abwägung zwischen den berechtigten Interessen der Strafverfolgungsbehörden an Telekommunikationsdaten und dem Schutz von Berufsgeheimnissen enthalte. Folgerichtig wurde der Entwurf abgelehnt und statt dessen die Geltungsdauer des § 12 FAG um zwei weitere Jahre verlängert (bis zum 31. Dezember 1999). Gleichzeitig wurde die Bundesregierung aufgefordert, bis zum 30. April 1998 einen neuen Entwurf als Nachfolgeregelung vorzulegen, der einen ausreichenden Schutz der Berufsgeheimnisse umfassen sollte. Die Bundesregierung hat jedoch mit der Begründung, es handele sich um eine vielschichtige und komplexe Thematik, die zur Zeit im Strafrechtsausschuß der Justizministerkonferenz geprüft werde, keinen neuen Vorschlag unterbreitet.

Ich werde mich in dieser Legislaturperiode nachdrücklich unter Beibehaltung meiner bisherigen Auffassung dafür einsetzen, diese Problematik sachgerecht zu lösen. Denn eines ist in den Beratungen im Zusammenhang mit § 12 FAG deutlich geworden: Diese Vorschrift entspricht nicht dem heutigen verfassungsgerichtlichen Verständnis von Wert und Bedeutung des Fernmeldegeheimnisses. Sie ist deshalb – zumal sie auch aus der Sicht der Bundesregierung novellierungsbedürftig ist – möglichst rasch durch eine neue Regelung zu ersetzen.

6.5 Einführung der Videotechnik bei Zeugenvernehmungen im Strafverfahren

In meinem letzten Tätigkeitsbericht (16. TB Nr. 6.3) hatte ich über Vorstellungen des Gesetzgebers berichtet, bei polizeilichen, staatsanwaltschaftlichen oder richterlichen Vernehmungen durch den Einsatz der Videotechnik zur Verbesserung des Opfer- und Zeugenschutzes beizutragen.

Durch das Gesetz zum Schutz von Zeugen bei Vernehmungen im Strafverfahren und zur Verbesserung des Opferschutzes – Zeugenschutzgesetz – (BGBl. 1998 I S. 820) wurden inzwischen Rechtsgrundlagen geschaffen, wonach die Aufzeichnung einer polizeilichen, staatsanwaltschaftlichen oder richterlichen Zeugenvernehmung auf Bild-Ton-Träger bei Personen unter sechzehn Jahren zulässig ist oder wenn Anlaß zur Sorge besteht, daß der Zeuge in der Hauptverhandlung nicht vernommen werden kann und die Aufzeichnung zur Erforschung der Wahrheit erforderlich ist. Für die Vernehmung in der Hauptverhandlung ist vorgesehen, daß der Vorsitzende des Gerichts bei der Vernehmung im Verhandlungssaal bleibt und er mit dem Zeugen, der sich in einem anderen Raum befindet, über eine Videodirektschaltung verbunden ist. Voraussetzung hierfür ist, daß das Wohl des Zeugen bei seiner Anwesenheit im Verhandlungssaal schwerwiegend benachteiligt würde.

In einer Vielzahl von Punkten stelle ich erfreulicherweise Übereinstimmung mit den Empfehlungen fest, die ich im Laufe der parlamentarischen Beratungen ausgesprochen habe. Hervorheben möchte ich dabei, daß die neuen Regelungen nicht nur kindlichen Opferzeugen, sondern auch anderen schutzbedürftigen Zeugen zugute kommen.

Die Entscheidungen über

- die Bild-Ton-Aufzeichnung zur Vermeidung immer neuer Vernehmungen und
- über die Bild-Ton- Direktübertragung der Vernehmung aus einem anderen Raum in den Verhandlungssaal

werden getrennt voneinander getroffen und unterliegen unterschiedlichen Voraussetzungen. Zu bemerken ist außerdem, daß die Bild-Ton-Aufzeichnung zum Zwecke des Zeugenschutzes keinen Einstieg für eine regelmäßige Video-Aufzeichnung zur Ablösung der sog. Verschriftung, also des herkömmlichen Protokolls, bedeutet.

Kritisch bewerte ich jedoch den Verzicht auf eine Regelung, die die Vervielfältigung von Bild-Ton-Aufzeichnungen untersagt oder zumindest limitiert. Ausgehend vom Zweck der Bild-Ton-Aufzeichnung, sie als Vernehmungsersatz (Vermeidung der Wiederholung) zu betrachten, hätte aus meiner Sicht unterbunden werden müssen, daß einzelne Prozeßbeteiligte bzw. deren Anwälte oder gar andere Personen an beliebigem Ort oder zu beliebiger Zeit das Videoband bzw. eine Kopie davon abspielen können. Auch fehlt es an wirksamen Vorkehrungen, die einen Mißbrauch verhindern könnten, wie z. B. einer sichtbaren Signierung des Videobandes oder strafbewährten Regelungen über die Zweckbindung. Ein weiterer Mangel des Zeugenschutzgesetzes ist, daß auf eine Einwilligung des Betroffenen zur Aufzeichnung verzichtet wurde. Wenn eine Bild-Ton-Aufzeichnung zum Schutz des Betroffenen gefertigt werden soll, so ist nach meiner Auffassung seine Einwilligung – nach vorheriger Aufklärung über die weitere Verwertung der Aufzeichnung – eine unverzichtbare Voraussetzung für deren Zulässigkeit. Die Datenschutzbeauftragten des Bundes und der Länder haben sich im Rahmen ihrer 54. Konferenz mit diesem Thema befaßt und Empfehlungen formuliert (s. Entschließung vom 23./24. Oktober 1997, **Anlage 10**).

In Zukunft wird die Frage im Vordergrund stehen, inwieweit moderne Dokumentationstechnik für die Wahrheitsfindung und den Zeugenschutz genutzt werden kann. Einer solchen Diskussion verschließe ich mich nicht, da die herkömmliche Art und Weise der Protokollierung häufig mit großen Mängeln behaftet ist. Dabei werde ich dafür eintreten, eine Lösung zu finden, die möglichst wenig in das Persönlichkeitsrecht des Betroffenen eingreift.

6.6 Reformen im Strafvollzug

Nachdem ich in den letzten Jahren wiederholt über notwendige Reformen des Strafvollzugsgesetzes (StVollzG) berichtet habe (zuletzt 16. TB Nr. 6.7), ist in der vergangenen Legislaturperiode erfreulicherweise die Novellierung des Gesetzes abgeschlossen worden. Damit wurden datenschutzrechtliche Bestimmungen in das Gesetz aufgenommen, die hinsichtlich des Rechts auf informationelle Selbstbestimmung der Strafgefangenen dringend erforderlich waren. Ich gehe davon aus, daß alsbald auch für die hiermit eng verbundenen Bereiche Untersuchungshaft und Jugendstrafvollzug gesetzliche Vorschriften verabschiedet werden, die vergleichbare datenschutzrechtliche Regelungen enthalten.

6.6.1 Viertes Gesetz zur Änderung des Strafvollzugsgesetzes

Mit dem Vierten Gesetz zur Änderung des Strafvollzugsgesetzes vom 26. August 1998 (BGBl. I S. 2461) ist das StVollzG nach langjährigen Bemühungen um bereichsspezifische Regelungen über den Schutz und die Verwendung personenbezogener Daten von Strafgefangenen ergänzt worden. Dabei mußte eine Balance zwischen datenschutzrechtlichen Erfordernissen und denen des Vollzugs gefunden werden. Wenngleich meine Empfehlungen nicht in allen Punkten berücksichtigt wurden, bin ich mit dem erzielten Kompromiß zufrieden. So konnte ich u.a. erreichen, daß bei der Überwachung von Telefongesprächen, die vor allem aus Gründen der Sicherheit oder Ordnung der Anstalt erfolgt (§ 32 i.V.m. § 27 StVollzG), die beabsichtigte Überwachung sowohl dem Gefangenen wie auch dem Gesprächspartner des Gefangenen nach Herstellung der Verbindung durch die Vollzugsbehörde oder den Gefangenen mitzuteilen ist. Der Gefangene kann damit frei darüber entscheiden, ob er ein Telefonat führen und damit seinem Gesprächspartner gegebenenfalls die Tatsache seiner Inhaftierung offenbaren will und, falls ja, mit welchem Inhalt er sein Gespräch führt. Steht ein Gefangener im Verdacht, vom Gefängnis aus Straftaten zu planen oder zu organisieren, gibt es diese Mitteilungspflicht nicht, vielmehr gelten die Voraussetzungen von § 100a StPO.

Für bedenklich halte ich die Regelung in § 182 Abs. 2 Satz 2 des Gesetzes, wonach Ärzte, Psychologen, Sozialarbeiter oder Pädagogen, also Personen, die ein Berufsgeheimnis zu schützen haben, personenbezogene Daten, die ihnen von einem Gefangenen als Geheimnis anvertraut oder über einen Gefangenen sonst bekannt geworden sind, dem Anstaltsleiter zu offenbaren haben, soweit dies für die Aufgabenerfüllung der Vollzugsbehörde oder zur Abwehr von erheblichen Gefahren für Leib oder Leben des Gefangenen erforderlich ist. Ich habe empfohlen, hier statt einer Mitteilungspflicht lediglich eine Offenbarungsbefugnis, d. h. einen Ermessensspielraum des Berufsgeheimnisträgers, vorzusehen, um eine Aushöhlung des Berufsgeheimnisses zu vermeiden. Ich hoffe, daß in der Praxis der Schutz der personenbezogenen Daten und das Vertrauensverhältnis zwischen den Gefangenen und dem genannten Personenkreis keinen Schaden nimmt.

Kritisch bewerte ich auch die Frage der Dauer der Aktenaufbewahrung. Die jetzt festgelegte Dauer von 20 Jahren für Gefangenenpersonalakten, Gesundheitsakten und Krankenblätter sowie von 30 Jahren für Gefangenenbücher halte ich für zu lang.

6.6.2 Gesetzentwurf über den Vollzug der Untersuchungshaft

Die Bemühungen des BMJ, in der vergangenen Legislaturperiode eine gesetzliche Regelung des Vollzugs der Untersuchungshaft vorzulegen, sind leider erfolglos

geblieben. Der mir zugeleitete vorläufige Referentenentwurf enthält zum Schutz des Persönlichkeitsrechts der Untersuchungshäftlinge, also Personen, die einer Straftat noch nicht überführt sind, unzureichende Vorschläge. In den Gesprächen mit dem BMJ habe ich u. a. deutlich gemacht, daß die geplante zwingende Kontrolle des Schriftwechsels von Gefangenen, die wegen Verdunklungsgefahr inhaftiert sind, nicht nur erheblich in das verfassungsrechtlich geschützte Briefgeheimnis des Inhaftierten, sondern eben auch in das seines Briefpartners eingreift. Auch bei Anerkennung der Regelungsmotive fordert der Grundsatz der Verhältnismäßigkeit, daß der Gefangene zumindest über die Rechtslage aufgeklärt wird. Ähnlich gelagert ist die Problematik bei der Überwachung der Telefongespräche (s. o. Nr. 6.6.1). Auch hier gebietet das informationelle Selbstbestimmungsrecht des Inhaftierten, ihn frühzeitig über die beabsichtigte Überwachung zu informieren. Auch und erst recht der Gesprächspartner des Gefangenen muß vor Beginn der Überwachungsmaßnahme hierüber sowie über die Tatsache informiert werden, daß die Überwachung auf der Inhaftierung des Gefangenen beruht. Ich werde mich bei den künftigen Beratungen dafür einsetzen, daß hier eine Lösung gefunden wird, die der neuen Vorschrift im StVollzG entspricht und somit datenschutzrechtlichen Anforderungen genügt.

6.6.3 Regelungen über den Jugendvollzug

Bedauerlicherweise ist es in der abgelaufenen Legislaturperiode auch nicht zu einer Reform des Jugendstrafvollzugs und der Untersuchungshaft von Jugendlichen gekommen, obwohl die Koalition dies laut ihrer Koalitionsvereinbarung *„unverzüglich in Angriff nehmen“* wollte. Ich halte dies unverändert für eine vordringliche Aufgabe und werde weiterhin auf gesetzliche Regelungen drängen.

6.7 Maßnahmen zur Korruptionsbekämpfung

In meinem 16. TB (Nr. 6.5) hatte ich über seitens der Bundesregierung vorgesehene Maßnahmen zur Korruptionsbekämpfung berichtet und insbesondere meine Sorge darüber ausgedrückt, daß die Straftatbestände der Bestechlichkeit und Bestechung in den Kreis derjenigen Tatbestände aufgenommen werden sollten, bei deren Verdacht eine Telefonüberwachung angeordnet werden darf. In den parlamentarischen Beratungen habe ich deutlich gemacht, daß der Korruption in Wirtschaft und Verwaltung zwar mit effektiven Mitteln entgegengetreten werden muß, diese aber mehr präventiven statt repressiven Charakter haben sollten. Das inzwischen in Kraft getretene Gesetz zur Bekämpfung der Korruption vom 13. August 1998 (BGBl. I S. 2038 ff) verzichtet auf eine Ausdehnung des Straftatenkatalogs, der eine Telefonüberwachungsmaßnahme auslösen kann. Der Gesetzgeber hat damit erfreulicherweise von einem weiteren Eingriff in Freiheitsrechte abgesehen und statt dessen Maßnahmen bevorzugt, die die informationelle Selbstbestimmung der Betroffenen schonen.

In ihrer Stellungnahme zu meinem 16. TB hat die Bundesregierung dennoch zum Ausdruck gebracht, daß sie das Anliegen unverändert für berechtigt hält, bei Bestechung und Bestechlichkeit die Telefonüberwachung zu ermöglichen. Aus meiner Sicht muß jedoch zunächst abgewartet werden, welchen Erfolg die präventiven Maßnahmen zeigen werden. Ein Schritt in die richtige Richtung sind die begleitend zum Korruptionsbekämpfungsgesetz von der Bundesregierung erlassenen Richtlinien zur Korruptionsprävention in der Bundesverwaltung. Diese Richtlinien konkretisieren die untergesetzlichen präventiven Maßnahmen und regeln, welche Vorbeugungsmaßnahmen von allen Dienststellen des Bundes zur Korruptionsverhinderung ergriffen werden sollen.

6.8 Zentrales Staatsanwaltschaftliches Verfahrensregister

Über die rechtlichen Grundlagen und Planungen zur Einrichtung eines länderübergreifenden zentralen staatsanwaltschaftlichen Verfahrensregisters (ZStV) bei dem Generalbundesanwalt beim Bundesgerichtshof – Dienststelle Bundeszentralregister – habe ich bereits mehrfach, zuletzt in meinem 16. TB (Nr. 6.9), ausführlich berichtet.

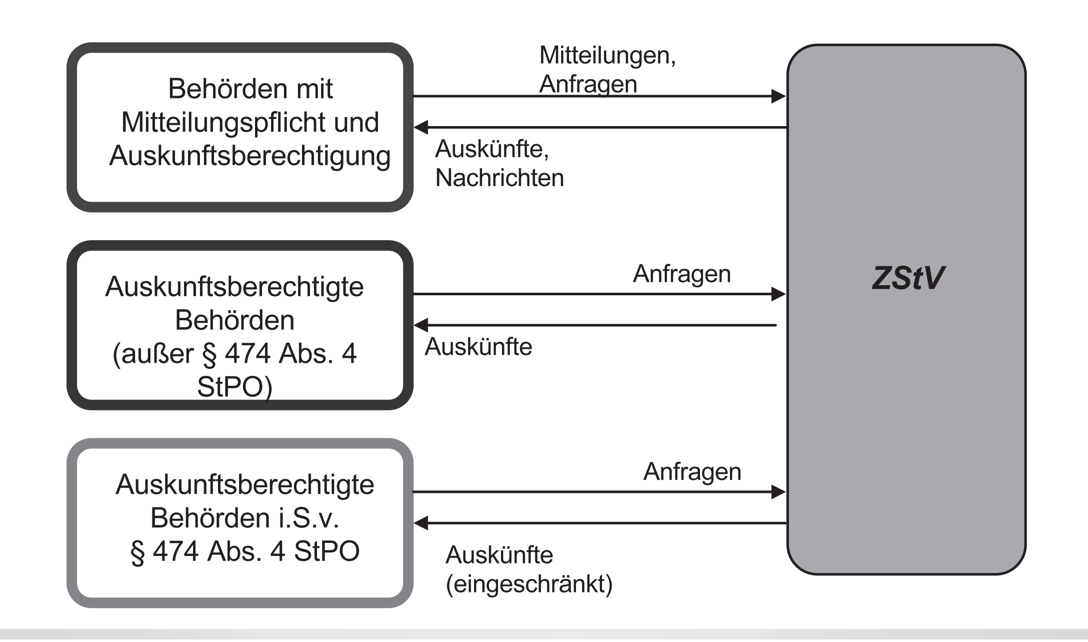
Im zurückliegenden Berichtszeitraum wurde die organisatorische und technische Umsetzung des Vorhabens eingeleitet. Die Realisierung erfolgte durch ein privates Unternehmen, das im Wege eines öffentlichen Ausschreibungsverfahrens unter mehreren Anbietern im November 1996 ausgewählt wurde. Dieses Unternehmen entwickelte auf der Basis der rechtlichen Vorgaben und des Leistungskataloges, die Bestandteil der Ausschreibung waren, ein Realisierungskonzept einschließlich der erforderlichen Software für den Betrieb des ZStV. Bereits während dieser Verfahrensentwicklung wurde ich durch das BMJ und den GBA beteiligt, so daß ich verschiedene datenschutzrechtliche Problemstellungen aufgreifen konnte. Besonderes Augenmerk habe ich dabei auf Fragen der Datenübermittlung, der Schnittstellen zum Bundeszentralregister, der Voraussetzungen, unter denen die Identitätsfindung des Betroffenen dem Datenempfänger überlassen werden darf (auch als „Ähnlichen-Service“ bezeichnet), des Sicherheitskonzeptes und der Verschlüsselungstechnik sowie des Outsourcing gelegt.

Durch das ZStV soll der schnelle Informationsaustausch zwischen den Strafverfolgungsbehörden gewährleistet und damit eine Zusammenfassung, Vereinfachung und Beschleunigung von Strafverfahren ermöglicht werden. Um dieses Ziel zu erreichen, sollen die Staatsanwaltschaften aller Bundesländer Personen- und Verfahrensdaten über ihre laufenden strafrechtlichen Ermittlungsverfahren an die Registerbehörde mitteilen und Auskünfte über alle in der Bundesrepublik anhängigen Verfahren gegen einen Beschuldigten einholen können. Das ZStV geht davon aus, daß pro Jahr ca. 6 Millionen Mitteilungen zu speichern sind, so daß – bei einer durchschnittlichen Speicherdauer von etwa fünf Jahren – mit einem Gesamtdatenbestand von ca. 30 Millionen Registereinträgen zu rechnen ist. Der Informationsfluß ist in der Abbildung 2 dargestellt.

Abbildung 2 (zu Nr. 6.8)



Informationsfluß (1)

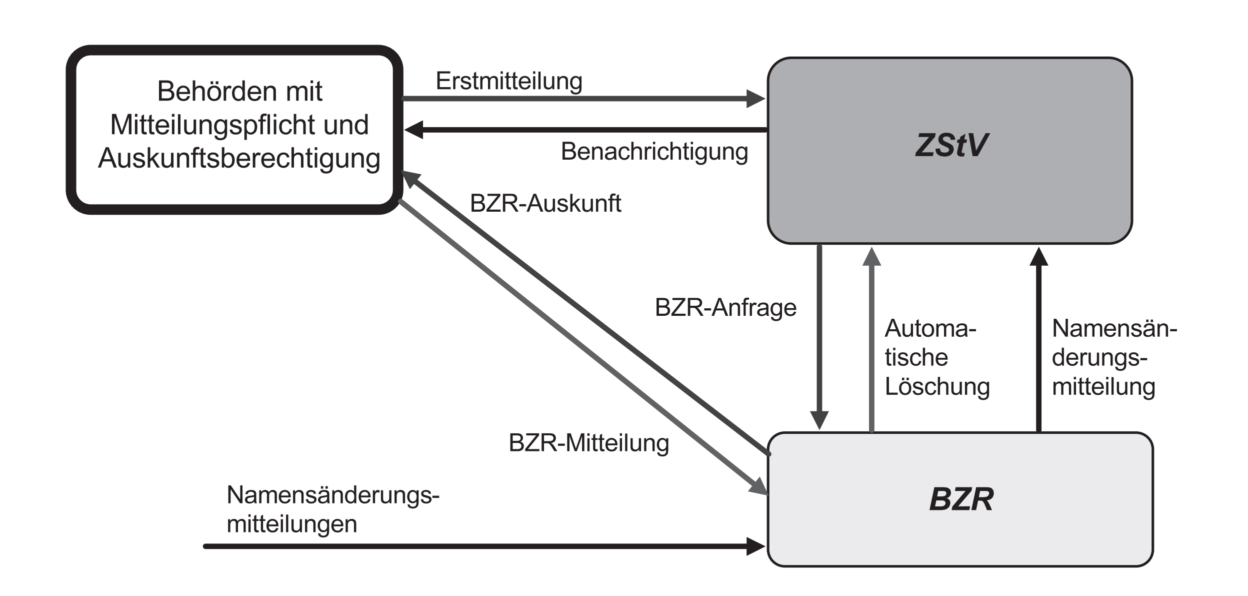


Verfahrensablauf und Datenstrukturen

Abbildung 3 (zu Nr. 6.8)



Informationsfluß (2)



Verfahrensablauf und Datenstrukturen

Ein wichtiger Punkt ist die Ausgestaltung der Schnittstellen zwischen dem ZStV und dem BZR. Das ZStV soll nämlich an das BZR, das ebenfalls vom GBA geführt wird, und in dem hauptsächlich rechtskräftige strafgerichtliche Verurteilungen gespeichert sind, angebunden werden. Mit einer Erstmitteilung zum ZStV kann dann die mitteilende Stelle gleichzeitig mit den mitgeteilten Personendaten eine Anfrage an das BZR stellen. In diesem Fall wird die Anfrage automatisch vom ZStV an das BZR weitergeleitet und wie eine direkte Anfrage an das BZR behandelt. Die BZR-Auskunft wird wie bisher als Ausdruck übersandt und nicht durch das ZStV erteilt. Bei Mitteilung eines auf Strafe erkennenden Urteils zum BZR wird der zugehörige Eintrag im ZStV automatisch gelöscht. Werden Namensänderungen zum BZR mitgeteilt, so löst dies auch im ZStV eine entsprechende Suche und ggf. eine Mitteilung an die auskunftsberechtigten Behörden aus. Dieser Informationsfluß ist in der Abbildung 3 dargestellt.

Ich habe besonderen Wert darauf gelegt, daß die Datenbanksysteme so gegeneinander abgeschottet sind, daß keine unzulässigen Verknüpfungen hergestellt werden können.

Für die Einrichtung des sog. Ähnlichen-Service (vgl. 16. TB Nr. 6.9) bei der Auskunftserteilung habe ich darauf hingewiesen, daß klare Abgrenzungen als Vorgaben für die Feststellung der Ähnlichkeit von Personendaten festgelegt sein müssen. Ich habe hier auf die Erfahrungen aus dem Aufbau und den Regelungen des Ausländerzentralregisters verwiesen. Wenngleich keine eigene gesetzliche Grundlage für diesen besonderen Abgleich geschaffen wurde, so sind nun in Anlehnung an die Regelungen im AZR-Gesetz für das ZStV eindeutige Kriterien als Filter für die Ähnlichensuche sowie für bestimmte Arten von Auskunftsersuchen vorgegeben.

Hinsichtlich des Sicherheitskonzeptes wurden getrennte Bedrohungs- und Risikoanalysen für die Aufbauphase und für die Betriebsphase erstellt, um spezifische Sicherheitskonzeptionen für den jeweiligen Entwicklungsstand implementieren zu können. Mit Beginn der Betriebsphase habe ich, gemeinsam mit dem BSI, die Verschlüsselung bei der Übermittlung der überaus schützenswerten, personenbezogenen Daten als unabweisbares Erfordernis festgestellt und seine Umsetzung vom BMJ gefordert. Allenfalls kann für eine Übergangszeit, in der noch an der Entwicklung eines geeigneten belastbaren Verschlüsselungssystems gearbeitet wird, eine niedrigere Sicherheitsstufe in Form einer „Geschlossenen Benutzergruppe“, in der alle Nutzer ausschließlich über denselben Telekommunikationsdiensteanbieter die Daten weitergeben, hingenommen werden.

M. E. sollte aber auch im Zuständigkeitsbereich der Länder verstärkt an der Einrichtung einer verschlüsselten Datenübermittlung vom und zum ZStV gearbeitet werden. Es ist davon auszugehen, daß die Kommunikation der Endnutzer mit dem ZStV über Kopf- oder Schnittstellen erfolgt, die in den Ländern eingerichtet werden. Diese Kopfstellen sammeln die an das ZStV zu versendenden Mitteilungen und Anfragen und sorgen für die Weiterleitung; umgekehrt werden die Auskünfte des ZStV an die Kopfstellen übermittelt, die sie dann an die ihr angeschlossenen Dienststellen weiterleiten. Das Tätigwerden der Kopfstellen liegt im Verantwortungsbereich der Länder. Ich halte es deswegen für notwendig, daß die gleich hohen Sicherheitsstandards, die zwischen dem ZStV und den Kopfstellen der Länder bestehen werden, auch darüber hinaus bis zum Endnutzer gewährleistet sind. Um dieses Sicherungskonzept zu erreichen, stehe ich mit den Landesbeauftragten für den Datenschutz in einem ständigem Dialog.

Das ZStV beabsichtigt, den operativen Betrieb einem Outsourcingnehmer zu übertragen. Damit ist aber keine Funktionsübertragung vorgesehen, die über rein technische Serviceleistungen hinausgeht. Insbesondere trägt die Registerbehörde die alleinige Verantwortung für das Gesamtverfahren und auch der komplette Bereich der Auskunftserteilung verbleibt in den Händen von ZStV-Mitarbeitern. Insofern habe ich, wenn auch noch die in anderen sicherheitsrelevanten Bereichen der öffentlichen Verwaltung bestehenden Vorgaben beachtet werden, keine Einwände erhoben. Dies gilt um so mehr, als die externe Vergabe lediglich als Übergangsstadium geplant ist. Nach Ablauf der Anlaufphase soll durch kontinuierliche Einarbeitung eigenes Personal mit der Wahrnehmung der Aufgaben vertraut gemacht werden, so daß nach Abschluß der Verlagerung der Dienststelle BZR von Berlin nach Bonn die Dienstleistungen durch ZStV-eigenes Personal erbracht werden. Der Wirkbetrieb soll am 1. April 1999 aufgenommen werden.

6.9 Novellierung des Bundeszentralregistergesetzes

Im 16. TB (Nr. 6.10) konnte ich darüber berichten, daß das BMJ endlich einen Entwurf zur Novellierung des Bundeszentralregistergesetzes (BZRG) vorgelegt hatte, der in vielen Bereichen meinen bereits seit Jahren wiederholt vorgetragenen Verbesserungsvorschlägen entsprach. Dazu zählten insbesondere

- der Wegfall der praktisch lebenslangen Eintragung einer einmal festgestellten Schuldunfähigkeit im Register,
- die Protokollierung aller erteilten Auskünfte und Hinweise durch die Registerbehörde,
- Vorschriften über ein automatisiertes Auskunftsverfahren und
- Regelungen der Auskunftserteilung für wissenschaftliche Forschungsvorhaben.

Zunächst schien es, daß die Novellierung des BZRG im Berichtszeitraum zügig vorankäme. Immer neue Entwürfe des BMJ ließen jedoch erkennen, daß allenfalls zum Ende der vergangenen Legislaturperiode die vage Hoffnung bestand, die dringend gebotenen Neuregelungen, wenn auch in stark gekürztem Umfang, in den parlamentarischen Gremien noch abschließend zu beraten. Diese Hoffnung hat sich letztlich leider nicht erfüllt. Ich gehe nunmehr davon aus, daß das Novellierungsvorhaben in dieser Legislaturperiode in seinem ursprünglichem Umfang umgesetzt werden wird.

6.10 Internationale Rechtshilfe in Strafsachen

Die wirtschaftlichen, gesellschaftlichen und politischen Veränderungen in Europa stellen die Sicherheitspolitik vor neue Herausforderungen, denen sowohl mit nationalen als auch mit international abgestimmten Maßnahmen begegnet werden muß. In diesem Zusammenhang kommt einer engen internationalen Zusammenarbeit der Strafverfolgungsbehörden und der Gerichte eine entscheidende Bedeutung zu.

Ich begrüße daher den „Entwurf eines Übereinkommens über die Rechtshilfe in Strafsachen zwischen den Mitgliedstaaten der Europäischen Union“, der dem Ziel der Verbesserung der justitiellen Zusammenarbeit in Strafsachen dient. Dadurch soll das bisherige Rechtshilfeübereinkommen vom 20. April 1959 ergänzt und die Rechtshilfe den Erfordernissen moderner grenzüberschreitender Strafverfolgung angepaßt werden. Vereinfachte Geschäftswege sollen die Bearbeitung von Rechtshilfeersuchen beschleunigen und grenzüberschreitende Ermittlungsmethoden eine rechtshilferechtliche Grundlage erhalten. Neue Vorschriften sollen auch die Überwachung von Telekommunikation erlauben.

Das Europäische Übereinkommen über die Rechtshilfe in Strafsachen aus dem Jahre 1959 enthält u. a. eine Regelung, der aus Sicht des Datenschutzes tragende Bedeutung zukommt. Diese Regelung (Artikel 2 lit. b) sieht vor, daß die Rechtshilfe gegenüber einem anderen Staat verweigert werden kann, wenn der ersuchte Staat der Ansicht ist, daß die Erledigung des Ersuchens geeignet ist, die Souveränität, die Sicherheit, die öffentliche Ordnung (ordre public) oder andere wesentliche Interessen seines Landes zu beeinträchtigen. In die gleiche Richtung zielt – wenn auch noch expliziter – eine weitere Vorschrift dieses Übereinkommens (Artikel 5 Abs. 1 lit. c). Danach kann bei Unterzeichnung oder Ratifizierung dieses Übereinkommens ein Erklärungsvorbehalt gemacht werden, der die Erledigung von Rechtshilfeersuchen um Durchsuchung oder Beschlagnahme von Gegenständen von der Vereinbarkeit des Ersuchens mit dem Recht des ersuchten Staates abhängig macht.

Diesen wichtigen Erklärungsvorbehalt hat die Bundesrepublik Deutschland bei der Hinterlegung der Ratifikationsurkunden erfreulicherweise gemacht.

Anläßlich der Beratungen des aktuellen Übereinkommensentwurfs darf es aber nicht dazu kommen, daß Gewährleistungen des Persönlichkeitsschutzes im deutschen Strafverfahrensrecht aufgegeben werden. Vielmehr sollte mit Nachdruck eine Annäherung, oder besser Angleichung strafverfahrensrechtlicher Vorschriften angestrebt werden, die unter datenschutzrechtlichen Gesichtspunkten den Vorbehalt der Vereinbarkeit mit dem Recht des ersuchten Staates überflüssig oder zumindest verzichtbar macht. Diese Bemühungen sollten nicht auf Rechtshilfeersuchen um Durchsuchungen oder Beschlagnahme von Gegenständen beschränkt sein. Die fortschreitende Entwicklung neuer Medien hat dazu geführt, Informationsinhalte nicht nur in herkömmlicher Weise, nämlich in „Gegenständen“, aufzubewahren, sondern zunehmend diesen neuen Kommunikationsdiensten anzuvertrauen. Es bedeutet somit keine Ausweitung des Persönlichkeitsschutzes zu Lasten der Durchsetzung des Strafanspruches eines Partnerstaates, sondern vielmehr eine Erhaltung des Interessenausgleichs in seiner früheren Substanz, wenn nunmehr datenschutzrechtliche Standards, die im Jahr 1959 noch ihren Schwerpunkt bei Durchsuchungen und Beschlagnahmen haben konnten, heute zusätzlich und besonders dort zu fordern sind, wo es um elektronische Überwachung geht.

In der Vergangenheit hat mich das BMJ bei den Beratungen des Entwurfs vereinzelt beteiligt. Vor der endgültigen Annahme dieses Entwurfs durch den Rat der Justiz- und Innenminister sind noch verschiedene Fragen zu klären, darunter auch die, ob und welche Datenschutzbestimmungen für die Übermittlung personenbezogener Daten im Rahmen der Rechtshilfe gelten. Da eine Aufnahme von Datenschutzbestimmungen in das Übereinkommen selbst nicht mehr möglich ist, strebt Deutschland deren Aufnahme in ein geplantes Zusatzprotokoll an. Die meisten anderen Mitgliedstaaten wollen aber lediglich unverbindlich prüfen, ob überhaupt ein Bedarf für Datenschutzbestimmungen besteht.

Den deutschen Vorschlag für eine Datenschutzbestimmung, der u. a. eine Zweckbindungsregelung vorsieht, nach der die Verarbeitung der personenbezogenen Daten durch den empfangenden Mitgliedstaat nur zum Zwecke der Strafverfolgung zulässig sein soll und eine Zweckänderung von der Zustimmung des übermittelnden Mitgliedstaats abhängig ist, unterstütze ich. Nachdem die Mitgliedstaaten in den Bereichen Polizei, Zoll und Asyl bereichsspezifische Datenschutzbestimmungen vereinbart haben, trete ich dafür ein, auch beim Rechtshilfeübereinkommen ein angemessenes Datenschutzniveau zu schaffen.

Darüber hinaus halte ich es für erforderlich, im Laufe dieser Legislaturperiode das Gesetz über internationale Rechtshilfe in Strafsachen zu novellieren und dem erforderlichen datenschutzrechtlichen Standards anzupassen.

6.11 Justizmitteilungen aus gerichtlichen und staatsanwaltlichen Verfahren

In meinen vorangegangenen Tätigkeitsberichten habe ich wiederholt auf die Notwendigkeit hingewiesen, eine gesetzliche Grundlage für Spontanmitteilungen der ordentlichen Gerichtsbarkeit und der Staatsanwaltschaften aus deren Verfahren an Gerichte, Behörden und sonstige öffentliche Stellen für andere Zwecke als die des Verfahrens zu schaffen (s. zuletzt 16. TB Nr. 6.13). Am 1. Juni 1998 ist nunmehr nach elfjähriger Entstehungszeit das „Justizmitteilungsgesetz und Gesetz zur Änderung kostenrechtlicher Vorschriften und anderer Gesetze – JuMiG –“ (BGBl. 1997 I S. 1430) in Kraft getreten.

Das JuMiG weist die Besonderheit auf, daß es für seine praktische Anwendung ergänzender Vorschriften bedarf. Auf der Grundlage der gesetzlichen Fallgruppen sind diejenigen Fälle im einzelnen festzulegen, in denen eine Mitteilung erforderlich ist und zu erfolgen hat. Obwohl von Seiten der Datenschutzbeauftragten immer wieder gefordert worden war, dies in Form von Rechtsverord-

nungen zu bestimmen, wurden dafür im Gesetz u. a. mit der Begründung eines verhältnismäßig häufigen Änderungsbedarfs allgemeine Verwaltungsvorschriften vorgesehen. Die bereits vor Inkrafttreten des JuMiG als allgemeine Verwaltungsvorschriften geltenden Anordnungen über Mitteilungen in Strafsachen (MiStra) und in Zivilsachen (MiZi) wurden entsprechend den Vorgaben des JuMiG neu gefaßt. Sie wurden nach der Verkündung des Gesetzes am 26. Juni 1997 von den Landesjustizministerien und dem BMJ binnen Jahresfrist überarbeitet. Mit den Landesbeauftragten für den Datenschutz habe ich zu den Entwürfen Stellung genommen. Die Neufassungen von MiStra und MiZi wurden in den jeweiligen Mitteilungsblättern der Länder und im Bundesanzeiger veröffentlicht (MiStra: BAnz 1998 Nr. 99a; MiZi: BAnz 1998 Nr. 138a).

Die Umsetzung des Gesetzes durch allgemeine Verwaltungsvorschriften ist letztlich vertretbar. Denn nach der Rechtsprechung des Bundesverfassungsgerichts müssen gesetzliche Vorschriften nur so bestimmt sein, wie dies nach der Eigenart der zu regelnden Sachverhalte mit Rücksicht auf den Normzweck möglich ist. Es genügt, daß die Betroffenen die Rechtslage erkennen und ihr Verhalten danach einrichten können (BVerGE 87, 234, 263).

In meinem 16. TB (Nr. 6.13) hatte ich zu zwei weiteren Punkten des damaligen Gesetzentwurfs Änderungsvorschläge unterbreitet. Da der Entwurf nicht klar genug erkennen ließ, bei welchen Fällen Mitteilungen zulässig und erforderlich sind, hatte ich darauf gedrungen, daß der Betroffene – wie bereits in einem Vorentwurf vorgesehen – grundsätzlich in jedem Falle einer Mitteilung über deren Inhalt und den Empfänger *von Amts wegen* unterrichtet wird. Mit der Begründung des hierfür erforderlichen Verwaltungsaufwands verblieb es aber bei der Regelung des Gesetzentwurfs, daß der Betroffene grundsätzlich erst *auf Antrag* die entsprechende Auskunft erhält (§ 21 EGGVG). In den parlamentarischen Beratungen wurde jedoch meinem Hinweis zugestimmt, daß der Betroffene dann zumindest möglichst rechtzeitig über sein Auskunftsrecht unterrichtet werden sollte.

Außerdem hatte ich mich darum bemüht, wegen der zum Teil erheblichen Auswirkungen einer Mitteilung für den Betroffenen eine Regelung im Gesetz selbst zu erreichen, wonach in bestimmten Fällen mit schwierigen Abwägungsfragen der Richter, der Staatsanwalt oder der Beamte des gehobenen Dienstes die Mitteilung im Einzelfall anordnet. Eine entsprechende – ebenfalls in dem vorangegangenen Gesetzentwurf vorgesehene – Vorschrift wurde zwar nicht in das JuMiG aufgenommen. In den Neufassungen von MiStra und MiZi finden sich aber entsprechende Regelungen (in der MiStra. z. B. Nrn. 2 und 3 Abs. 2 und 15 Abs. 3 Satz 4; in der MiZi z. B. Nrn. 3 Abs. 3 und 11 Abs. 2).

Insgesamt gesehen ist es erfreulich, daß nach jahrelangen Bemühungen nunmehr mit dem JuMiG eine gesetzliche Grundlage für die zahlreichen Übermittlungen personenbezogener Daten aus Verfahren der ordentlichen Gerichtsbarkeit und der Staatsanwaltschaften an andere öffentliche Stellen vorliegt und auch mit den Neufassungen von MiStra und MiZi angemessene Vorschriften geschaffen worden sind.

6.12 Bereichsspezifischer Datenschutz bei Notaren

Im 16. TB (Nr. 6.15) hatte ich berichtet, daß es mir nicht möglich war, im Regierungsentwurf für ein Drittes Gesetz zur Änderung der Bundesnotarordnung und anderer Gesetze eine datenschutzgerechte Formulierung der darin vorgesehenen Änderung des § 1 Abs. 5 Rechtsberatungsgesetz zu erreichen. In dem Entwurf war vorgesehen, daß Gerichte und Behörden der für die Entscheidung zuständigen Stelle grundsätzlich personenbezogene Daten übermitteln dürfen, die für die Rücknahme oder den Widerruf der Erlaubnis oder zur Einleitung eines Rügeverfahrens „von Bedeutung sein können“. Mein Anliegen war es, die Schwelle für die Zulässigkeit solcher Mitteilungen entsprechend den datenschutzrechtlichen Anforderungen anzuheben und genauer dahingehend festzulegen, daß die jeweiligen personenbezogenen Daten nur übermittelt werden dürfen, wenn sie für die Aufgabenerfüllung der Empfängerbehörde erforderlich sind.

Inzwischen ist das Dritte Gesetz zur Änderung der Bundesnotarordnung und anderer Gesetze verkündet worden (BGBl. 1998 I S. 2585). Im Laufe der Beratungen des Rechtsausschusses des Deutschen Bundestages habe ich erfreulicherweise erreichen können, daß Datenübermittlungen nicht nur im Rahmen des § 1 Abs. 5 Rechtsberatungsgesetz erst dann zugelassen werden, wenn sie „aus der Sicht der übermittelnden Stelle erforderlich sind“. Darüber hinaus wurden auf meine Anregung hin die entsprechenden Regelungen des § 64a Abs. 3 Satz 1 Bundesnotarordnung mit diesem Gesetz und des § 36a Abs. 3 Satz 1 Bundesrechtsanwaltsordnung sowie des § 32a Abs. 3 Satz 1 Patentanwaltsordnung mit dem Gesetz zur Änderung der Bundesrechtsanwaltsordnung, der Patentanwaltsordnung und anderer Gesetze (BGBl. 1998 S. 2600) ebenso geändert. Gleichzeitig wurden in diesen Vorschriften entsprechend der Terminologie des BDSG und der EG-Datenschutzrichtlinie die Worte „Belange“ durch „Interessen“ ersetzt. Die vorgenommenen Änderungen bewirken weitgehend nur terminologische Korrekturen. Aber auch Regelungen mit datenschutzrechtlichem Inhalt erfordern eindeutige und klare Formulierungen.

7 Finanzwesen

7.1 Das Bundesamt für Finanzen gab keine Auskunft über Freistellungsaufträge – Bürgerrechte wurden einfach ignoriert!

Das Bundesamt für Finanzen (BfF) hat zu prüfen, ob die Auftraggeber von Freistellungsaufträgen die Grenzen der steuerlichen Freibeträge nicht unzulässig überschreiten (s. 14. TB Nr. 6.2). Zu diesem Zweck melden die Banken, Sparkassen und vergleichbare Institute dem BfF einmal jährlich für das vorangegangene Jahr die Namen und Anschriften der Auftraggeber und die Höhe, über die die Freistellungsaufträge jeweils erteilt worden sind.

Vielfach bitten Auftraggeber das BfF um Auskunft über ihre dort zu ihren Freistellungsaufträgen gespeicherten Daten, etwa weil sie wegen eines Wohnungswechsels, durch Änderung der Bankverbindung(en) oder aus ande-

ren Gründen die Übersicht über die von ihnen erteilten Freistellungsaufträge verloren haben oder auch, weil sie nachprüfen wollen, ob die über sie gespeicherten Angaben zutreffen. Nach Mitteilung des BfF sind beispielsweise von Januar bis Ende August 1998 rund 530 schriftliche und weitaus mehr telefonische Anfragen eingegangen.

Aufgrund eines Erlasses des BMF vom 14. April 1997 wurde jedoch die Auskunft im wesentlichen jeweils unter Berufung auf § 45d Abs. 2 EStG verweigert, wonach die Mitteilungen der Banken und der anderen Stellen über erteilte Freistellungsaufträge *„ausschließlich zur Überprüfung der rechtmäßigen Inanspruchnahme des Sparer-Freibetrages und des Pauschbetrages für Werbungskosten verwendet werden“* dürfen.

Seither wandten sich immer wieder Betroffene wegen der Verletzung ihres Anspruchs auf Auskunft an mich. Noch häufiger war dies der Fall, seit die Arbeitsämter im Rahmen der Überprüfung des bei der Arbeitslosenhilfe zu berücksichtigenden Vermögens auch nach den Freistellungsaufträgen der Antragsteller fragen (s. u. Nr. 20.2). So schrieb mir ein Bürger:

> *„Mit diesem Brief erbitte ich Ihre Hilfe. Denn es ist kaum logisch, daß von mir Daten erhoben werden – dann bei Anfrage die Auskunft versagt wird. Selbst die Zivilprozeßordnung und die Strafprozeßordnung gestatten die Einsichtnahme in sensiblere Daten, um fehlerhaft erhobene oder vorgehaltene Informationen gegebenenfalls berichtigen zu können“.*

Andere Petenten machten ihrer Verärgerung noch deutlicher Luft.

Allerdings hatte inzwischen auch das Finanzgericht Köln in einem – nicht rechtskräftigen – Urteil vom 25. Juni 1998 den Anspruch eines Betroffenen auf Auskunft über seine im Zusammenhang mit seinen Freistellungsaufträgen gespeicherten Daten abgelehnt. Das Gericht begründete dies damit, die Mißbrauchskontrolle des BfF nach § 45d EStG werde gefährdet, wenn dem betroffenen Steuerpflichtigen die dort gesammelten Daten mitgeteilt würden. Das Kontrollverfahren sei nach der Darstellung des beklagten BfF so ausgestaltet, daß es im Wege des „Ähnlichkeitsrasters“ dem naheliegenden Mißbrauch vorbeuge, durch geringfügige Änderungen eines Datensatzes (Name oder Geburtsdatum) die datenbankgestützte Erfassung von Mehrfachfreistellungen zu verhindern. Dieser Mechanismus würde unterlaufen, wenn dem Steuerpflichtigen die Feststellung möglich wäre, ob Manipulationen erfolgreich waren oder nicht. Die Ausführungen des BfF müsse das Gericht dahin verstehen, daß eine Auskunft auch die Mitteilung von Ergebnissen des „Ähnlichkeitsrasters“ bedeuten würde.

Nach meiner Auffassung haben die Auftraggeber jedoch gegenüber dem BfF einen Anspruch auf Auskunft nach § 19 BDSG.

Das BMF berief sich demgegenüber – wie dargelegt – auf § 45d Abs. 2 EStG, um die Auskunft zu verweigern. Es verkannte den Sinn und Zweck dieser Vorschrift. Denn das Auskunftsrecht der Auftraggeber von Freistellungsaufträgen wird darin überhaupt nicht angesprochen. Die Anordnung des Gesetzgebers, daß das BfF die bei ihm gespeicherten Daten nur zur Prüfung der rechtmäßigen Inanspruchnahme des Sparer-Freibetrages und des Pauschbetrages für Werbungskosten verwenden darf, läßt die Frage unberührt, ob es dem Betroffenen gegenüber zur Auskunft über seine Daten verpflichtet ist. § 45d Abs. 2 EStG legt lediglich fest, inwieweit das BfF über die ihm anvertrauten Daten von sich aus verfügen darf. Das in § 45d Abs. 2 EStG gewählte Wort *„verwenden“* umfaßt hierbei jegliche Form des Verarbeitens und Nutzens der Daten. Der Begriff bezieht sich jedoch nur auf den begrenzten Sachverhalt der Prüfung dieser Daten.

Auch das für das vorgenannte Urteil des Finanzgerichts Köln maßgebliche Argument, durch entsprechende Anfragen könne das Kontrollsystem gefährdet werden, überzeugte nicht. Da nur ein Anspruch auf Auskunft besteht, soweit die Angaben des Anfragenden mit den gespeicherten Daten identisch sind, können Datensätze, die den Daten des Fragestellers lediglich ähnlich sind, nicht ausgeforscht werden. Das „Ähnlichkeitsraster“ darf dem Betroffenen gerade nicht mitgeteilt werden. Dann ist aber auch keine Gefahr ersichtlich, daß das Kontrollsystem des § 45d EStG unterlaufen wird.

Ich habe die Verweigerung der Auskünfte gegenüber dem BMF **beanstandet**.

Mit einer Entschließung der 56. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 5./6. Oktober 1998 (**s. Anlage 16**) haben mich meine Kollegen aus den Ländern nachdrücklich in meiner Forderung an das BMF unterstützt, den Erlaß an das BfF vom 14. April 1997 aufzuheben und dieses anzuweisen, dem Auskunftsanspruch der Auftraggeber von Freistellungsaufträgen nachzukommen. Ich habe die Entschließung dem Bundesminister der Finanzen mit der Bitte zugeleitet, sich der Sache anzunehmen.

Das BMF hat mir nunmehr mitgeteilt, daß es den o. g. Erlaß vom 14. April 1997 durch Erlaß vom 5. Januar 1999 ersetzt hat. Hiernach hat das BfF *„nach pflichtgemäßem Ermessen einem Freistellungsauftraggeber Auskunft über die im Rahmen des Kontrollverfahrens nach § 45 d EStG über ihn gespeicherten Daten zu erteilen, soweit der Freistellungsauftraggeber hierfür ein berechtigtes Interesse darlegt oder dies ohne weitere Ermittlungen ersichtlich ist und keine Versagungsgründe vorliegen“.* Die Auskunft ist zu versagen, soweit überwiegende schutzwürdige Interessen Dritter (z. B. § 30 AO) entgegenstehen, der Kontrollzweck gefährdet werden könnte oder die Erteilung von Auskünften einen unverhältnismäßigen Aufwand erfordern würde.

Das BMF teilt allerdings nach wie vor nicht meine Auffassung, daß der Auskunftsanspruch sich aus § 19 BDSG ergibt. Es stützt sich allgemein auf das Recht auf informationelle Selbstbestimmung und sieht dies in Konkurrenz zu dem verfassungsrechtlich verankerten Auftrag an den Rechtsstaat, die Besteuerung gleichmäßig durchzuführen (Artikel 3 GG). Es verweist darauf, das informationelle Selbstbestimmungsrecht und der Auftrag zur gleichmäßigen Besteuerung müßten im jeweiligen Kernbereich erhalten bleiben.

In der neuen Regelung des BMF sehe ich vor allem eine pragmatische Lösung, die im Ergebnis dem Anliegen der Betroffenen sehr weitgehend Rechnung trägt, die Aus-

künfte zu erhalten, die ihnen nach meiner Auffassung gemäß § 19 BDSG zustehen. Insofern begrüße ich den Erlaß des BMF vom 5. Januar 1999. Die Praxis muß allerdings zeigen, ob insbesondere die in § 19 BDSG nicht – aber im Erlaß – enthaltene Voraussetzung, daß ein berechtigtes Interesse darzulegen ist, zur Versagung der Auskunft in Fällen führt, in denen diese nach § 19 BDSG zu erteilen wäre.

Ich bedauere, daß das BMF nicht den Auskunftsanspruch des Freistellungsauftraggebers aufgrund des § 19 BDSG anerkennt, der in seinem Absatz 4 auch Regelungen dafür trifft, wann die Auskunft zu versagen ist. Diesem Punkt, der im Einzelfall Bedeutung gewinnen kann, werde ich weiter nachgehen. Entscheidend ist jedoch für mich zunächst, daß dem Anliegen der Betroffenen auf Auskunft in der Praxis nunmehr zumindest sehr weitgehend entsprochen werden kann. Die Petenten, die sich an mich gewandt haben, habe ich von diesem erfreulichen Ergebnis unterrichtet.

7.2 Steuerliche Fahrtenbücher – Unzulässige Offenbarung von Patientendaten

Um die ertragsteuerliche Behandlung der privaten Kfz-Nutzung zu vereinfachen, wurde im Jahressteuergesetz 1996 festgelegt, daß der private Nutzungsanteil eines zum Betriebsvermögen des Steuerpflichtigen gehörenden Kraftfahrzeugs pauschal mit monatlich 1 v.H. des Anschaffungswertes zu berücksichtigen ist. Bei Steuerpflichtigen, die ihr Fahrzeug nur in geringem Umfang privat nutzen, kann dies zu einer unzutreffend überhöhten Bewertung des privaten Nutzungsanteils führen. Wenn sie dies vermeiden wollen, müssen sie daher von der Möglichkeit des § 6 Abs. 1 Nr. 4 Satz 3 EStG Gebrauch machen und zum Nachweis des tatsächlichen Verhältnisses der betrieblichen zu den privaten Fahrten ein Fahrtenbuch führen. In meinem 16. TB (Nr. 7.3) habe ich berichten können, daß nach Mitteilung des BMF bei Ärzten, die regelmäßig Hausbesuche machen, im Fahrtenbuch der Vermerk *„Patientenbesuch"* mit Ortsangabe genügt. Damit waren zunächst meine datenschutzrechtlichen Bedenken ausgeräumt, die sich aus der grundsätzlich für alle betroffenen Berufsgruppen geltende Anforderung der allgemeinen Grundsätze des BMF ergaben, *„aufgesuchte Geschäftspartner"* im Fahrtenbuch zu bezeichnen (BStBl 1997 I S. 562 ff., 564).

Durch Eingaben besorgter Bürger wurde mir Ende 1997 jedoch bekannt, daß das BMF mit Schreiben vom 1. August 1997 an die Bundesärztekammer festgelegt hatte, die erwähnten allgemeinen Grundsätze seien auch von den Ärzten ohne Einschränkung zu beachten. Soweit Ärzte bislang nur den Vermerk *„Patientenbesuch"* und den Ort ihrer Tätigkeit in das Fahrtenbuch eingetragen hätten, könnten sie zwar bis zum 31. Dezember 1997 weiterhin so verfahren. Danach hätten aber auch sie den aufgesuchten Patienten *„als Geschäftspartner ... genau zu bezeichnen"*. Ansonsten sei das Fahrtenbuch nicht ordnungsgemäß im Sinne des § 6 Abs. 1 Nr. 4 Satz 3 EStG geführt. Die Nutzung des betrieblichen Fahrzeugs für private Fahrten werde dann nach den Pauschsätzen bewertet.

Diese im Einvernehmen mit den obersten Finanzbehörden der Länder getroffene Festlegung führt dazu, daß Ärzte, die ein Fahrtenbuch führen, um ungerechtfertigte steuerliche Nachteile zu vermeiden, entgegen § 102 Abs. 1 Nr. 3c AO mit dessen Vorlage bei der Finanzbehörde die Namen und Anschriften der von ihnen aufgesuchten Patienten offenbaren müssen und folglich auch gegen § 203 Abs. 1 Nr. 1 StGB verstoßen, der den Bruch der ärztlichen Schweigepflicht unter Strafe stellt. Ich habe dies mit dem BMF eingehend erörtert, um zu erreichen, daß es seine Regelung wieder aufhebt und zum früheren Verfahren zurückkehrt. Meine Bemühungen blieben jedenfalls bisher leider ohne Erfolg.

Die Forderung des BMF, daß Ärzte die Namen und Anschriften der von ihnen aufgesuchten Patienten im Fahrtenbuch angeben, halte ich für rechtswidrig:

1. § 102 Abs. 1 Nr. 3c AO räumt den Ärzten das Recht ein, insoweit die Auskunft zu verweigern. Das BMF weist zwar zutreffend darauf hin, daß die finanzielle Sicherheit des Staates und die Gleichmäßigkeit der Besteuerung öffentliche Interessen mit Verfassungsrang sind und die Finanzverwaltung verpflichtet ist, die Angaben der Steuerpflichtigen zu überprüfen. Zu diesem Zweck fordert es die Namen und Anschriften der Patienten. Die Pflicht der Beteiligten nach § 93 Abs. 1 Satz 1 AO zur Auskunft über den für die Besteuerung erheblichen Sachverhalt unterliegt jedoch – wie das Bundesverfassungsgericht (HFR 1989 S. 440f.) ausdrücklich bestätigt hat – entsprechend dem Verhältnismäßigkeitsgrundsatz neben anderen Beschränkungen den Grenzen der §§ 102 ff. AO. Damit wird – bei berechtigter Auskunftsverweigerung – eine Einschränkung der Sachaufklärung in Kauf genommen. Das öffentliche Interesse tritt insoweit zurück. Dem Schutz des jeweils in Frage stehenden Vertrauensverhältnisses wird der Vorrang eingeräumt.

   Die hier maßgebliche Vorschrift des § 102 Abs. 1 Nr. 3c AO dient der Wahrung der ärztlichen Schweigepflicht als einer wesentlichen Grundlage des Vertrauensverhältnisses zwischen Arzt und Patient. Die Regelung gibt dem Arzt ein Auskunftsverweigerungsrecht für alles, was ihm *„in dieser Eigenschaft anvertraut oder bekanntgeworden ist"*. Hierzu zählen auch der Name und die Anschrift des Patienten, wie der Bundesgerichtshof für die gleichgelagerte Vorschrift des § 53 Abs. 1 Nr. 3 StPO entschieden hat (BGHSt 33, 148 ff., 151). Der Arzt muß sich frei entscheiden können, ob er sein Auskunftsverweigerungsrecht ausüben will oder ob er sich zur Auskunft entschließt. Die Finanzbehörden dürfen ihn bei seiner Entscheidung nach § 102 Abs. 1 Nr. 3 c AO nicht beeinflussen. Das BMF mißachtet jedoch diese Vorgabe des Gesetzgebers mit seiner Forderung, die aufgesuchten Patienten in dem Fahrtenbuch stets genau zu bezeichnen.

2. Nach § 203 Abs. 1 Nr. 1 StGB ist der Bruch der ärztlichen Schweigepflicht strafbar.

   Entgegen der Auffassung des BMF gibt insbesondere § 93 Abs. 1 Satz 1 AO dem Arzt nicht die Befugnis, stets und ohne eigene freie Abwägung die Namen und

Anschriften der von ihm aufgesuchten Patienten zu offenbaren. § 93 Abs. 1 Satz 1 AO ist im Hinblick auf das Auskunftsverweigerungsrecht des Arztes auf ein bloßes Fragerecht reduziert. Nur das Ergebnis der freien Abwägung des Arztes, ob er seiner Schweigepflicht nachkommen oder sie aus besonderen Gründen durchbrechen will, nicht aber § 93 Abs. 1 Satz 1 AO könnte möglicherweise im Einzelfall eine Offenbarung von Patientendaten rechtfertigen.

Die vom BMF allgemein aufgestellte Forderung, die aufgesuchten Patienten in dem Fahrtenbuch genau zu bezeichnen, damit es als ordnungsgemäß geführt anerkannt werden könne, nimmt dem Arzt die Möglichkeit der freien Entscheidung, wenn er nicht in bestimmten Fällen ungerechtfertigte steuerliche Nachteile in Kauf nehmen will. Damit setzt das BMF zumindest die Ärzte der Gefahr einer Bestrafung nach § 203 Abs. 1 Nr. 1 StGB aus, die nach Abwägung der in Frage stehenden Interessen zu dem Ergebnis gelangen, eine Durchbrechung ihrer Schweigepflicht sei nicht gerechtfertigt, dann aber dennoch im Hinblick auf die vom BMF getroffene Regelung die Namen und Anschriften der von ihnen aufgesuchten Patienten in das Fahrtenbuch eintragen und die Daten mit dessen Vorlage bei der Finanzbehörde Dritten unbefugt offenbaren.

Inzwischen habe ich die vom BMF mit dem Schreiben an die Bundesärztekammer getroffene Regelung gegenüber dem BMF **beanstandet**. Eine abschließende Stellungnahme lag mir bei Redaktionsschluß nicht vor. Die derzeitigen Gespräche mit dem BMF lassen eine jedenfalls pragmatische Lösung erwarten.

7.3 Keine datenschutzrechtliche Überarbeitung der Abgabenordnung in Sicht

In meinem 16. TB (Nr. 7.1) hatte ich über die sehr kontrovers geführte Diskussion mit Vertretern des BMF und der obersten Finanzbehörden der Länder über meine Vorschläge zur datenschutzrechtlichen Verbesserung der Abgabenordnung berichtet. In seiner inzwischen vorliegenden Stellungnahme vertritt das BMF die Auffassung, es sei weder rechtlich erforderlich noch wünschenswert, die Mehrzahl meiner Vorschläge aufzugreifen.

Das BMF führt im wesentlichen zunächst grundsätzlich aus:

Bereits die Abgabenordnung 1919 habe eine Vorschrift über das Steuergeheimnis enthalten und die Erhebung der Daten geregelt. Es erscheine fraglich, ob die Rechtsprechung des Bundesverfassungsgerichts zum Volkszählungsgesetz, die maßgeblich für die Umschreibung des Rechts auf informationelle Selbstbestimmung gewesen sei, ohne weiteres auf den Bereich der Steuerverwaltung übertragbar sei. Dies zeige auch der im BDSG festgelegte Vorrang bereichsspezifischer Vorschriften (§ 1 Abs. 4). Inwieweit die Grundsätze des Volkszählungsurteils auf die überwiegend dem wirtschaftlichen Bereich zuzurechnenden Daten der Finanzverwaltung angewendet werden könnten, habe das Bundesverfassungsgericht in seinem Zinsurteil (BVerfGE 84, 239) selbst aufgeworfen. Es habe eine endgültige Bewertung jedoch offengelassen und darauf hingewiesen, daß die dort beanstandeten Vorschriften der Abgabenordnung ohnehin den datenschutzrechtlichen Grundsätzen entsprächen.

Weder das Bundesverfassungsgericht noch der Bundesfinanzhof hätten bisher Vorschriften der Abgabenordnung aus datenschutzrechtlicher Sicht beanstandet. Das Bundesverfassungsgericht habe im Gegenteil Vorschriften der Abgabenordnung ausdrücklich oder inzident als verfassungsmäßig angesehen (§ 30 „im Grundsatz, verfassungskonform“, §§ 93 Abs. 1, 194 Abs. 3, 208 Abs. 1 AO). Man könne allenfalls erwägen, die Abgabenordnung aus Zweckmäßigkeitsgründen zu präzisieren. Jede Änderung des Wortlauts werfe jedoch die Frage auf, ob eine inhaltliche Rechtsänderung gewollt sei. Damit werde auch fraglich, ob die auf den bisherigen Wortlaut bezogene Rechtsprechung noch berücksichtigt werden könne oder Makulatur sei. Es sei dann eine Flut von Prozessen zu erwarten.

Vor diesem Hintergrund erklärt dann das BMF gegenüber den einzelnen Vorschlägen zur Ergänzung und Präzisierung der Abgabenordnung u. a., sie seien weder rechtlich erforderlich noch zweckmäßig, sie seien bereits seit Jahrzehnten geltendes Recht (Vorschläge zu § 30 AO), die kritisierte Vorschrift sei verfassungskonform (Vorschlag zu § 88a AO), der Vorschlag laufe dem gesetzgeberischen Willen zuwider (Vorschlag zu § 105 AO), die jetzige Regelung habe eine Vielzahl von Vorteilen (Vorschlag zu § 184 Abs. 3 AO) oder für eine Präzisierung und Schaffung weiterer Rechtsgrundlagen für die Erhebung, Verarbeitung und Nutzung bestehe kein Anlaß (Vorschlag zu § 208 AO). Auch die Einfügung eines Abschnitts „Datenschutz“ sei abzulehnen, weil sie mit einer völligen Neufassung der Abgabenordnung verbunden wäre und hierfür kein praktischer Nutzen ersichtlich sei.

In Abstimmung mit den Landesbeauftragten für den Datenschutz habe ich das BMF darauf hingewiesen, daß eine Abwägung der schutzwürdigen Interessen der Steuerpflichtigen und der Verpflichtung der Finanzbehörden, die Steuern gleichmäßig festzusetzen, erforderlich sei. Gegenüber der gegenwärtigen Entwicklung liege es im beiderseitigen Interesse, durch bereichsspezifische Datenschutzregelungen auf der Grundlage etwa meiner Vorschläge die Abgabenordnung aus datenschutzrechtlicher Sicht zu verbessern.

Ferner habe ich das BMF darauf aufmerksam gemacht, daß wegen der technischen Entwicklung im Bereich der automatisierten Datenverarbeitung Vorkehrungen zum Schutz des Steuergeheimnisses zu treffen sein werden, die den damit verbundenen neuen Risiken für die Persönlichkeitsrechte der betroffenen Steuerpflichtigen wirksam begegnen können. Angesichts der Öffnung neuer Informations- und Kommunikationstechniken auch für die Steuerfestsetzung sowie der sich abzeichnenden Möglichkeiten des Internet zur elektronischen Kommunikation sowohl der Finanzbehörden untereinander als auch mit den Steuerpflichtigen dürften künftig besondere datenschutzrechtliche Vorkehrungen notwendig werden. Auch sei festzustellen, daß eine immer größere Bereitschaft bestehe, Steuerdaten für andere – steuerfremde – Zwecke zu verwenden. Nicht zuletzt mache es aber auch

die anstehende Umsetzung der EG-Datenschutzrichtlinie in nationales Recht erforderlich, die Abgabenordnung aus der Sicht des Datenschutzes zu überprüfen und gegebenenfalls zu überarbeiten.

Weiterhin habe ich darauf hingewiesen, daß sich das Bundesverfassungsgericht in seiner Entscheidung zum Flick-Untersuchungsausschuß auf sein für den Datenschutz grundlegendes Volkszählungsurteil bezogen (BVerfGE 67, 100, 143) und es ausdrücklich offengelassen hat, ob alle Tatbestände des § 30 AO den verfassungsrechtlichen Anforderungen an den Schutz individualisierter und individualisierbarer steuerlicher Daten genügen (a.a.O. S. 144). Auch berücksichtige der Bundesfinanzhof in seinen Erwägungen zu den Grenzen zulässiger Kontrollmitteilungen datenschutzrechtliche Grundsätze (Urteil vom 18. Februar 1997, NJW 1997, S. 2067, 2072).

Abschließend habe ich gegenüber dem BMF verdeutlicht, daß die Vorstellungen der Datenschutzbeauftragten über Verbesserungen des Datenschutzes in der Abgabenordnung mit seiner Stellungnahme sicher nicht gegenstandslos geworden seien.

Der 13. Deutsche Bundestag hat bei der Beratung meines 16. TB (Nr. 7.1) bereits zur Kenntnis genommen, *„daß die Bundesregierung gegenwärtig die Vorschläge des Bundesbeauftragten für den Datenschutz für Änderungen der Abgabenordnung unter datenschutzrechtlichen Gesichtspunkten nicht übernimmt“*. Er hat seine Erwartung zum Ausdruck gebracht, *„daß die Bundesregierung im Einzelfall datenschutzrechtliche Empfehlungen zur Abgabenordnung auch künftig sorgfältig prüft und erforderliche Änderungen aufgreift“* (Empfehlungen des Innenausschusses, Drucksache 13/11168 vom 23. Juni 1998, vom Plenum angenommen in der 243. Sitzung am 24. Juni 1998).

7.4 Automatisiertes Abrufverfahren für Steuerdaten

Der Versuch des BMF, eine **Steuerdaten-Abruf-Verordnung** zu erlassen, hatte zunächst nicht zum Erfolg geführt, nachdem ihm der Bundesrat wegen Bedenken der kommunalen Spitzenverbände im Hinblick auf die Bedürfnisse und Möglichkeiten der Gemeinden den Verordnungsentwurf zurückgegeben und gebeten hatte, die Probleme nochmals zu erörtern (16 TB Nr. 7.2). Daraufhin hat das BMF – gewissermaßen als kleinere Lösung – gemeinsam mit den obersten Finanzbehörden der Länder zunächst den Text des Verordnungsentwurfs aktualisiert und eine Steuerdaten-Abruf-Verwaltungsregelung erarbeitet (BStBl I 1998, S. 1205), die nicht für die Gemeinden gilt.

Inzwischen hat allerdings der Deutsche Städtetag das BMF – auch für die Bundesvereinigung der kommunalen Spitzenverbände – unterrichtet, daß man einer Rechtsverordnung mit den in der Steuerdaten-Abruf-Verwaltungsregelung festgelegten Anforderungen an automatisierte Abrufe von Steuerdaten zustimmen werde. Das BMF bereitet daher auf der Grundlage der Steuerdaten-Abruf-Verwaltungsregelung nunmehr einen neuen Entwurf für eine Steuerdaten-Abruf-Verordnung vor.

Bei der Erarbeitung der Steuerdaten-Abruf-Verwaltungsregelung ist das BMF nicht meiner Empfehlung gefolgt vorzuschreiben, daß die abgerufenen Daten bei der Übertragung kryptographisch verschlüsselt werden. Es verwies darauf, daß eine Einwahl in die Standleitungen zwischen den Finanzämtern und den Rechenzentren von Dritten, also Personen oder Stellen, die nicht für die Standleitungen zugelassen wurden, nicht möglich sei, so daß sich eine Verschlüsselung erübrige. Für den künftigen Abruf von Daten über öffentlich zugängliche Übertragungsnetze werde die Möglichkeit einer Verschlüsselung – gegebenenfalls nach einer Übergangsfrist – aber erneut geprüft werden. Da derzeit ein entsprechendes länderübergreifendes Verschlüsselungsverfahren entwickelt wird (s. Nr. 8.6), werde ich meine Empfehlung spätestens bei der Erörterung des neuen Entwurfs für eine Steuerdaten-Abruf-Verordnung jedoch wieder aufgreifen.

Insgesamt sehe ich es als erfreulich an, daß mit der wohl in absehbarer Zeit zu erwartenden Steuerdaten-Abruf-Verordnung – nach dem derzeitig sinnvollen Zwischenschritt einer Steuerdaten-Abruf-Verwaltungsregelung – doch noch eine gesetzliche Grundlage mit denselben Anforderungen für Abrufe von Steuerdaten in Bund, Ländern und Gemeinden vorliegen wird.

7.5 Änderung der Mitteilungsverordnung – Nicht alle Zweifel ausgeräumt

Im Entwurf einer Zweiten Änderungsverordnung zur **Mitteilungsverordnung** ist vorgesehen, eine Rechtsgrundlage für regelmäßige Mitteilungen von Zollbehörden an Landesfinanzbehörden über gewährte Ausfuhrerstattungen zu schaffen (Artikel 1 § 4a). In meinem 16. TB (Nr. 7.4.2) habe ich meine Bedenken hiergegen geäußert, da das BMF diese Regelung nur mit dem allgemeinen Hinweis auf § 85 AO und damit begründet hatte, die Mitteilungen seien sowohl im Veranlagungsverfahren als auch bei Außen- und Betriebsprüfungen erforderlich, um feststellen zu können, ob die Empfänger diese Zahlungen vollständig als Betriebseinnahmen erfaßt haben.

Auf meinen erneuten Vorbehalt hat das BMF nunmehr erläutert, die Mitteilung sämtlicher Ausfuhrerstattungen sei erforderlich, da die Einnahmen aus diesen variablen Subventionen erfahrungsgemäß in vielen Fällen bei den Steuererklärungen nicht angegeben würden. Andere wirkungsvolle Kontroll- und Ermittlungsmöglichkeiten stünden der Finanzverwaltung hinsichtlich der gewährten Ausfuhrerstattungen nicht zur Verfügung. Unter Berufung auf das sog. Zinsurteil des Bundesverfassungsgerichts (BVerfGE 84, 239, 273) legte das BMF dar, daß erhöhte Anforderungen an die Steuerehrlichkeit des Steuerpflichtigen gestellt würden, wenn die Steuerfestsetzung – wie hier – von dessen Erklärung abhinge. Der Gesetzgeber müsse deshalb die Steuerehrlichkeit durch hinreichende – die steuerliche Belastungsgleichheit aller Steuerpflichtigen gewährleistende – Kontrollmöglichkeiten abstützen. Insofern bedürfe das Deklarationsprinzip der Ergänzung durch das Verifikationsprinzip.

Ich hätte es vorgezogen, meine Bewertung nicht nur auf die allgemeine Mitteilung von Erfahrungen über die An-

gabe von Ausfuhrerstattungen in Steuererklärungen stützen zu müssen, sondern auch auf konkrete Zahlen, etwa über den Anteil insoweit nicht korrekter Steuererklärungen oder über die Höhe von Beträgen hierdurch bedingter Steuerausfälle. Gleichwohl hat mir das BMF – vor allem in Verbindung mit den von ihm herangezogenen Ausführungen des Bundesverfassungsgerichts in dessen Zinsurteil – mit seiner Antwort bestätigt, daß der Eingriff in das Persönlichkeitsrecht der Empfänger von Ausfuhrerstattungen im Interesse der Allgemeinheit vertretbar ist. Insofern habe ich meine Bedenken zurückgezogen.

In dem Entwurf ist weiterhin eine Mitteilungspflicht der Bundesanstalt für Arbeit (BA) gegenüber den Finanzbehörden vorgesehen. Die BA soll hiernach bestimmte Daten ausländischer Unternehmen (Namen und Anschrift des Unternehmens, Beginn, Dauer und Ort der Durchführung des Werkvertrages) mitteilen, die aufgrund bilateraler Regierungsvereinbarungen über die Beschäftigung von Arbeitnehmern zur Ausführung von Werkverträgen tätig werden (Artikel 1 § 6 Abs. 2). Zunächst hatte der Text des Entwurfs nicht berücksichtigt, daß die BA nach der gesetzlichen Ermächtigung zum Erlaß der vorliegenden Regelung in einer Rechtsverordnung nur zur Mitteilung u.a. von Verwaltungsakten oder von Angaben hieraus verpflichtet werden darf und daß auch nur Daten ausländischer Unternehmen übermittelt werden dürfen (§§ 93a AO, 71 Abs. 1 Satz 1 Nr. 3 SGB X). Hierauf habe ich das BMF mit Unterstützung des BMJ hingewiesen. Der vom BMF daraufhin überarbeitete Entwurf sieht jetzt zutreffend vor, daß nur Daten der ausländischen Unternehmen mitzuteilen sind, also nicht z. B. Namen und Anschriften der inländischen Vertragspartner. Auch die Eingrenzung der Übermittlungen auf Daten aus Verwaltungsakten ist jetzt vorgesehen. Die genaue Formulierung hierfür ist zwar noch offen. Entscheidend ist für mich aber, daß die vom Gesetzgeber gezogenen Grenzen der Mitteilungspflicht nach übereinstimmender Auffassung nunmehr eingehalten werden.

7.6 Inter- und supranationale Zusammenarbeit

7.6.1 Endlich Mustertext für EG-Drittlandsabkommen über die Amtshilfe im Zollbereich

In zurückliegenden Tätigkeitsberichten (14. TB Nr. 6.7.2, 15. TB Nr. 5.7 und 16. TB Nr. 7.9.5) habe ich einige datenschutzrechtliche Fragen beim Austausch personenbezogener Informationen aufgrund von Zollzusammenarbeitsabkommen der EG mit Drittstaaten dargestellt. Das federführende BMF hatte mich an den Vorarbeiten zu den Amtshilfeprotokollen regelmäßig beteiligt und meine Empfehlungen weitgehend aufgegriffen. Allerdings war es in der Vergangenheit oft schwierig, sich in der zuständigen Arbeitsgruppe des Europäischen Rates auf ausreichende und einheitliche Datenschutzvorkehrungen zu einigen und sie mit dem jeweiligen Vertragspartner zu vereinbaren.

Ich begrüße es daher sehr, daß die Ratsgruppe sich inzwischen über einen Mustertext für Amtshilfeabkommen im Zollbereich verständigt hat, der neben der Verpflichtung zur Wahrung des Amtsgeheimnisses und zur Einhaltung der Zweckbindung vorsieht, daß personenbezogene Daten nur ausgetauscht werden dürfen, wenn der empfangende Staat ein Schutzniveau gewährleistet, das dem des übermittelnden Staats mindestens gleichwertig ist. Der Mustertext erfüllt damit im Ergebnis die Anforderungen des Artikel 25 Abs. 1 EG-Datenschutzrichtlinie, wonach personenbezogene Daten in ein Drittland regelmäßig nur übermittelt werden dürfen, wenn dieses Land ein angemessenes Datenschutzniveau gewährleistet.

In jüngster Zeit hat mir das BMF allerdings mitgeteilt, daß es dennoch im Einzelfall (z. B. bei dem Abkommen mit Hongkong) schwierig bleibt, darauf hinzuwirken, daß die EG den intern vorgesehenen Standard mit dem jeweiligen Vertragspartner dann auch wirklich vereinbart. Ich habe dem BMF mit Hinweis auf Artikel 25 Abs. 1 EG-Datenschutzrichtlinie empfohlen, einer Unterschreitung der im Mustertext vorgesehenen datenschutzrechtlichen Vorkehrungen im Interesse der Betroffenen nicht zuzustimmen. Das BMF hat meine Empfehlung aufgegriffen. Ich hoffe, daß die von der EG mit Drittstaaten abgeschlossenen Abkommen auch künftig jedenfalls den von der Richtlinie geforderten Mindeststandard für den Austausch personenbezogener Daten vorsehen werden.

7.6.2 Noch keine datenschutzgerechte Umsetzung der „Schwarze Liste"-Verordnung

In den Mitgliedstaaten der EU und bei der Europäischen Kommission ist auf der Grundlage der Verordnung (EG) Nr. 1469/95 des Rates vom 22. Juni 1995 über Vorkehrungen gegenüber bestimmten Begünstigten der vom EAGFL (Europäischer Ausrichtungs- und Garantiefonds für die Landwirtschaft), Abteilung Garantie, finanzierten Maßnahmen (ABl. EG Nr. L 145/1 vom 29. Juni 1995) ein Identifikations- und Mitteilungssystem (Schwarze Liste) eingerichtet worden. Es soll bei Marktbeteiligten, bei denen das Risiko der Unzuverlässigkeit besteht, verstärkte Kontrollen und ggf. zusätzliche Maßnahmen ermöglichen. Die Führung der „Schwarzen Liste" ist der Zentralstelle Betrugsbekämpfung (ZEB) beim Hauptzollamt Hamburg-Jonas übertragen worden.

Datenschutzrechtliche Probleme, die sich bei der Umsetzung der genannten Verordnung in der Praxis ergeben, habe ich in meinem 16. TB (Nr. 7.9.3) beschrieben. Vor allem geht es darum sicherzustellen, daß nicht auf Daten Marktbeteiligter direkt zugegriffen werden kann, auf die die Verordnung (noch) nicht anzuwenden ist, weil die festgestellten Unregelmäßigkeiten den Schwellenwert von 100 000 ECU nicht überschreiten. Hierzu habe ich dem BMF nach einer Beratung der Oberfinanzdirektion Hamburg und der ZEB vorgeschlagen, eine Datenbank zu erstellen, in die die Daten zu Marktbeteiligten, die den Schwellenwert (noch) nicht erreichen, zwar über eine Maske eingegeben werden können, aber für einen direkten Zugriff nicht verfügbar sind. Erst bei Überschreiten des Schwellenwertes sollten die betreffenden Datensätze automatisch in die „Schwarze Liste" übernommen oder nach Ablauf der Verjährungsfrist nach manuellem Anstoß ohne Kenntnisnahme gelöscht werden.

Das BMF hat hiergegen eingewandt, mein Vorschlag halte den Anforderungen der ZEB nicht Stand, weil diese ohne einen direkten Zugriff *„keinen Überblick*

über den aktuellen Sachstand" habe und *„keine Auskünfte mehr an das BMF"* erteilen könne. Außerdem würden in die Liste *„auch Firmen aufgenommen, gegen die vorerst nur ein Verdacht"* bestehe. Falls dieser sich als unbegründet erweise, müsse eine unverzügliche Löschung dieser Daten möglich sein. Schließlich müßten eventuelle Eingabefehler stets im direkten Zugriff korrigierbar bleiben.

Die Einwände des BMF haben mich bislang nicht überzeugt. Eine Verarbeitung oder Nutzung der Daten Marktbeteiligter, auf die die Verordnung (noch) nicht anwendbar ist, kann nur zur Überwachung des Schwellenwertes innerhalb des Verjährungszeitraums zulässig sein. Die vom BMF dargelegten datenverarbeitungstechnischen Probleme sind m. E. ohne unverhältnismäßig großen Aufwand zu lösen.

Das BMF hat mir seine Bereitschaft angezeigt, gemeinsam nach einer angemessenen Lösung zu suchen.

7.7 Datenverarbeitung bei Familienkassen (Kindergeld)

Das Kindergeld wird seit dem 1. Januar 1996 – von bestimmten Fällen nach dem Bundeskindergeldgesetz abgesehen – als Steuervergütung nach dem Einkommensteuergesetz gezahlt. Die hierfür zuständigen Familienkassen bei den Arbeitsämtern, den öffentlichen und einigen privaten Arbeitgebern, wie z. B. der Deutschen Post AG, sind Finanzbehörden (s. § 5 Abs. 1 Nr. 11 Finanzverwaltungsgesetz). Sie unterliegen der Fachaufsicht des Bundesamtes für Finanzen.

7.7.1 Mißverständliche Anforderung von Nachweisen durch Familienkassen

Ein Petent wandte sich an mich, weil die Familienkasse eines Arbeitsamts in einem Schreiben an ihn verlangt hatte, zum Nachweis über das Ende des Studiums seines Sohnes „zum Beispiel Kopie des Diplomzeugnisses" vorzulegen. Er machte geltend, die darin enthaltenen Zeugnisnoten seien für die Gewährung des Kindergeldes ohne jegliche Bedeutung. Das als vorgesetzte Behörde des Bundesamtes für Finanzen von mir um Stellungnahme gebetene BMF stimmte mit mir überein, daß die Auffassung des Petenten zutrifft. Es verwies jedoch auf das den Kindergeldberechtigten regelmäßig ausgehändigte Kindergeld-Merkblatt. Darin werde erläutert, daß bei der Vorlage von Prüfungszeugnissen als Nachweis für den Tag der Beendigung der Ausbildung *„darin enthaltene Beurteilungen und Benotungen ... unkenntlich"* gemacht werden könnten. Ein Prüfungszeugnis mit Noten sei somit nicht angefordert worden.

Bei den Kindergeldberechtigten können allerdings durchaus Zweifel auftreten, ob die allgemeinen Ausführungen eines Merkblatts noch gelten sollen, wenn eine Familienkasse konkret im Einzelfall in einem Schreiben von einem Betroffenen ohne einschränkenden Hinweis fordert, ein bestimmtes Zeugnis vorzulegen. Deshalb hatte ich dem BMF empfohlen, auch in den Schreiben der Familienkassen, in denen nach Zeugnissen gefragt wird, jeweils auf die Möglichkeit hinzuweisen, daß Beurteilungen und Benotungen unkenntlich gemacht werden können. Das BMF hielt dies unter Berufung auf das Kindergeld-Merkblatt zunächst nicht für erforderlich.

Ein weiterer Petent wandte sich aus demselben Grunde an mich. Auch hier forderte die Familienkasse eines Arbeitsamts, zum Nachweis des Abschlusses der Ausbildung das Diplomzeugnis des Kindes vorzulegen, und sie lehnte es auch noch ab, statt dessen eine entsprechende Bescheinigung der Ausbildungsstätte entgegenzunehmen. Diese Möglichkeit des Nachweises war aber ebenso ausdrücklich in dem Kindergeld-Merkblatt genannt. Außerdem stellte sich heraus, daß der Petent das Kindergeld-Merkblatt nicht erhalten hatte.

Daraufhin habe ich dem BMF erneut empfohlen, daß Familienkassen unabhängig von dem Kindergeld-Merkblatt in Schreiben mit Anforderungen von Zeugnissen auf die Möglichkeit hinweisen, Beurteilungen und Benotungen unkenntlich zu machen.

Das BMF antwortete zwar, das Bundesamt für Finanzen sei bisher davon ausgegangen, daß auch die Familienkassen die im Merkblatt gegebenen Informationen in ihrer Arbeitspraxis z. B. bei der Anforderung von Nachweisen umsetzen und daß Unstimmigkeiten zwischen Aussagen im Kindergeld-Merkblatt und der Verfahrensweise einer Familienkasse im direktem Kontakt geklärt würden. Das Bundesamt für Finanzen hat aber nunmehr gleichwohl in einem Rundschreiben an die Familienkassen ausdrücklich darauf hingewiesen, daß die Informationen des Kindergeld-Merkblattes auch von den Familienkassen anzuwenden sind. Beim Nachweis eines Ausbildungsendes sei z. B. darauf zu achten, daß dies sowohl durch Abschlußzeugnis als auch durch eine Bestätigung des Ausbildungsinstitutes geschehen kann. Hinsichtlich der Abschlußzeugnisse sollten die Berechtigten darauf hingewiesen werden, daß Noten geschwärzt werden können (BStBl I 1998 S. 1126).

Damit dürften – wenn auch erst nach einigen Schwierigkeiten – die Voraussetzungen dafür geschaffen sein, daß bei der Vorlage von Nachweisen für den Abschluß der Ausbildung des Kindes künftig bei den Kindergeldberechtigten Zweifel über den Umfang des Nachweises und bei den Familienkassen gegebenenfalls auch überflüssige Datenerhebungen vermieden werden.

7.7.2 Gefährdete Geheimhaltung einer Adoption

Durch die Eingabe eines Kindergeldbeziehers wurde ich darauf aufmerksam gemacht, daß Mitbürger gegenüber öffentlichen Stellen Angaben manchmal bewußt zurückhalten, um dadurch schützenswerte Geheimnisse zu wahren. Dies kann allerdings das Gegenteil bewirken.

Der Petent hatte vor Jahren zusätzlich zu seinen leiblichen Kindern ein weiteres Kind adoptiert. Zuvor hatte dieses Kind bereits einige Zeit in dessen Familie zur Pflege gelebt. Da Pflegeeltern auch für ein Pflegekind kindergeldberechtigt sind, hatte der Petent für sein Pflegekind unter dessen damaligem Familiennamen beim zuständigen Arbeitsamt Kindergeld beantragt und auch erhalten. Kurz nachdem der Petent und seine Frau das Kind adoptiert hatten, zog er mit seiner Familie in eine andere, entfernt gelegene Stadt. Dort erhielt er vom nunmehr zuständigen Arbeitsamt Kindergeld. Auf dem

alle sechs Jahre auszufüllenden Haushaltsfragebogen bezeichnete er sein Adoptivkind stets als „leibliches Kind“. Der Petent teilte dem Arbeitsamt nicht mit, daß das Kind inzwischen adoptiert worden war, da er der Ansicht war, daß es das nunmehr zuständige Arbeitsamt nichts angehe, daß es sich nicht um ein leibliches, sondern um ein Adoptivkind handele. Um so größer war die Überraschung, als er kurz vor dem 18. Geburtstag des Adoptivkindes von der Familienkasse des Arbeitsamtes angeschrieben und ihm mitgeteilt wurde, daß die Kindergeldzahlungen für das Kind – es folgte der Vorname des Kindes und der Familienname, mit dem das Kind geboren wurde – eingestellt würden, wenn nicht rechtzeitig die Voraussetzungen für die Weiterzahlung des Kindergeldes über das 18. Lebensjahr hinaus nachgewiesen würden. Der Petent fragte sich, wie das Arbeitsamt den Familiennamen erfahren hat, mit dem das Adoptivkind geboren wurde, obwohl er dem Arbeitsamt gegenüber niemals diesen Namen genannt und das Kind immer als „leibliches Kind“ bezeichnet hatte.

Offensichtlich war der Petent davon ausgegangen, daß das Arbeitsamt, in dessen Bezirk er bislang lebte, die Kindergeldakte nach einem Umzug schließt und das jetzt zuständige Arbeitsamt einen neuen Vorgang anlegt. Dem ist jedoch nicht so. Vielmehr übersendet das bisher zuständige Arbeitsamt die von ihm angelegte Kindergeldakte an das nach dem Umzug zuständige Arbeitsamt, das die Kindergeldakte lediglich weiterführt. Darüber hinaus werden bei jedem Antrag auf Zahlung von Kindergeld die Daten über den Kindergeldberechtigten und über das Kind, für das Kindergeld gezahlt wird, an eine Zentraldatei bei der Bundesanstalt für Arbeit gemeldet. Im vorliegenden Fall waren also die Angaben, einschließlich des Familiennamens, den das Kind zum Zeitpunkt seiner Geburt trug, in der Zentraldatei der Bundesanstalt für Arbeit gespeichert worden. Da der Petent die Familienkasse (früher: Kindergeldkasse) des Arbeitsamtes niemals über die erfolgte Adoption und die damit verbundene Änderung des Geburtsnamens nach § 1757 Abs. 1 BGB informiert hatte, galt das Kind für die Arbeitsverwaltung bei der Bearbeitung des Kindergeldes ungeachtet der Bezeichnung als „leibliches Kind“ in den Haushaltsfragebogen weiterhin als Pflegekind.

Um zu verhindern, daß die Tatsache der Adoption etwa durch ein Schreiben der Familienkasse weiteren Personen bekannt würde, hätte der Petent die Familienkasse hierüber unterrichten müssen. Hierzu wäre er nach § 60 des Ersten Buches Sozialgesetzbuch (SGB I) und den für das Kindergeld geltenden Vorschriften (bis zum 31. Dezember 1995 das Bundeskindergeldgesetz, nunmehr § 68 Abs. 1 EStG) verpflichtet gewesen.

Dem Petenten hat es daher nicht nur nicht geholfen, dem Arbeitsamt gegenüber zu verschweigen, daß er sein Pflegekind mittlerweile adoptiert hatte. Vielmehr hat er damit maßgeblich zu der Möglichkeit beigetragen, daß die Tatsache, die er geheimhalten wollte, unbeabsichtigt weiteren Personen offenbart wird. Die Beachtung von Mitteilungspflichten gegenüber öffentlichen Stellen liegt nicht immer nur in deren Interesse, sondern nicht selten auch im Interesse des betroffenen Bürgers.

8 Wirtschaft und Informationsgesellschaft

8.1 Informations- und Kommunikationsdienste-Gesetz

Mit dem am 1. August 1997 in Kraft getretenen Informations- und Kommunikationsdienste-Gesetz (IuKDG) wurden Regeln geschaffen, die angesichts der entstehenden Informationsgesellschaft einen angemessenen Umgang mit den neuen Medien sicherstellen können, weil sie die Interessen aller Beteiligten ausgleichend berücksichtigen. Dabei kommt dem Datenschutz eine besondere Bedeutung zu, die auch die Enquete-Kommission in ihrem Schlußbericht zur „Zukunft der Medien in Wirtschaft und Gesellschaft – Deutschlands Weg in die Informationsgesellschaft“ (Drucksache 13/11004) hervorhebt und durch weiterreichende Maßnahmen im technischen und rechtlichen Bereich gestützt sehen möchte.

Gegen die im Entwurf des Teledienstedatenschutzgesetzes (TDDSG) vorgesehene Verpflichtung der Diensteanbieter, auf Verlangen Bestandsdaten ihrer Kunden insbesondere an Nachrichtendienste zu übermitteln (s. u. Nr. 10.1.5.3), hatte ich Bedenken erhoben (vgl. 16. TB Nrn. 1.5 und 8.1). Denn von den Möglichkeiten der neuen Netze gehen keine solchen Gefahren aus, als daß zusätzlich zu den ohnehin geltenden Vorschriften, z. B. der Strafprozeßordnung oder denjenigen für die Datenerhebung durch die Nachrichtendienste, noch besondere Auskunftspflichten der Diensteanbieter hätten geschaffen werden müssen. Und für die Urheber von in Deutschland verbotenen extremistischen oder verfassungsfeindlichen Äußerungen besteht die Möglichkeit, in Staaten auszuweichen, die solche Betätigungen nicht als strafbar ansehen; ein bekanntes Mittel, sich der Verfolgung zu entziehen, ohne an Wirksamkeit im Inland einzubüßen. Zusätzliche Auskunftspflichten der Diensteanbieter wären aber von vielen Nutzern als Risiko empfunden worden, jederzeit unter eine besondere Aufsicht zu geraten. Sie hätten zudem die Bereitschaft gemindert, sich frei zu informieren und selbst eine Meinung zu äußern. Es ist erfreulich, daß diese Regelung im Rahmen der parlamentarischen Diskussion des Entwurfs gestrichen wurde.

Zu meinem Bedauern ist es aber bei der Streichung des Datenschutz-Audit aus dem TDDSG geblieben (vgl. 16. TB Nrn. 1.5 und 8.1). Inzwischen hat sich jedoch bei vielen die Erkenntnis durchgesetzt, daß ein entsprechendes Qualitätssiegel die Akzeptanz der neuen Medien fördern kann und daß es dazu hilfreich wäre, wenn durch gesetzliche Rahmenbedingungen die Vertrauenswürdigkeit eines Qualitätssiegels und der in ihm enthaltenen Zusicherungen verbürgt wäre. Solche Rahmenbedingungen werden derzeit in einem Projekt erarbeitet (s. u. Nr. 8.2.2).

Die Evaluierung des IuKDG wurde mit der Fachveranstaltung des BMBF „Informations- und Kommunikationsdienste-Gesetz – Umsetzung und Evaluierung – Chancen für die Wirtschaft, Erwartungen an Verwaltung und Gesetzgebung“ im Dezember 1997 auf eine breite Basis gestellt. Mehrere Arbeitskreise mit unterschied-

lichen Themenschwerpunkten wurden beauftragt, Erfahrungen und Probleme bei der Umsetzung des IuKDG zusammenzustellen und auszuwerten.

Im Arbeitskreis „Datenschutz“ werden die Erfahrungen der Aufsichtsbehörden, der Wirtschaft und der Verbraucher mit dem TDDSG zusammengetragen und in einem Bericht verdichtet, der am Ende der Evaluierungsphase im Sommer 1999 vorgelegt wird. Insgesamt bestätigen die bisherigen Erfahrungen der Aufsichtsbehörden meine eigenen Beobachtungen (s. u. Nr. 8.2.1). Ohne dem Evaluierungsbericht vorgreifen zu wollen, sind erhebliche Startschwierigkeiten bei der Umsetzung des TDDSG bei allen Beteiligten festzustellen. Viele der vorhandenen Probleme lassen sich jedoch durch die begonnene Zusammenarbeit lösen, andere durch die Etablierung einer entsprechenden Sicherheitsinfrastruktur. Daher erscheint es mir notwendig, den Aufbau einer solchen Infrastruktur durch entsprechende Projekte – auch im nicht-öffentlichen Bereich – zu unterstützen.

Aus meiner Beteiligung am Arbeitskreis „Digitale Signaturen“ kann ich berichten, daß zahlreiche Firmen die Anerkennung als Zertifizierungsstelle beantragt haben, von denen nach der TeleSec noch weitere im Laufe des Jahres 1999 zugelassen werden und dann am Markt zur Verfügung stehen. Daher liegen praktische Erfahrungen bisher noch nicht vor (s. u. Nr. 8.7). Wesentliche Voraussetzung für den umfassenden Einsatz der digitalen Signatur ist die Rechtssicherheit für alle Beteiligten. Sobald die Erfahrungen es rechtfertigen, sollte deshalb die rechtliche Gleichstellung der elektronischen mit der eigenhändigen Unterschrift erfolgen, die für den weltweiten Einsatz durch internationale Anerkennungsabkommen auf der Basis harmonisierter Gesetze und Verfahren hergestellt werden müßte.

8.2 Umgang mit Nutzerdaten

8.2.1 Deutsche Diensteanbieter im Dornröschen-Schlaf?

Bei den Telediensten werden zwei Arten von Diensten unterschieden:

Informations- und Dienstleistungsangebote, wie z. B. Wetter- oder Börsendaten, Reise- und Warenangebote, und die Zugangsvermittlung zu solchen Diensten über das Internet.

Vornehmlich die großen Diensteanbieter **(Service Provider)**, wie AOL, Compuserve und T-Online, bieten außer dem Zugang zum Internet auch eigene Informationen und Dienstleistungen an. Daneben gibt es mittlerweile auch mehrere Hundert kleinere regionale Provider, die im wesentlichen nur den Zugang zum Internet anbieten.

Voraussetzung für den Zugang zum Internet ist ein Vertrag mit einem Zugangs-Provider, der die dafür nötige technische Ausrüstung bereithält. Für den Vertragsabschluß verlangen die Provider entsprechend der gesetzlichen Vorgabe in § 5 Abs. 1 Teledienstedatenschutzgesetz (TDDSG) nur die erforderlichen personenbezogenen Daten wie Name, Vorname, Adresse, Geburtsdatum und ggf. Telefonnummer. Die in wenigen Fällen darüber hinausgehenden Angaben sind als optional gekennzeichnet. Das TDDSG schreibt den Diensteanbietern außerdem vor, die Nutzer **vor der Erhebung** der Daten über Art, Umfang, Ort und Zweck der Erhebung und Verarbeitung ihrer Daten zu **unterrichten**, auch wenn der Rahmen der gesetzlich erlaubten Verarbeitung nicht überschritten wird. Für diese Unterrichtung bieten sich die Allgemeinen Geschäftsbedingungen (AGB) oder der Vertrag selbst an.

Das Ergebnis meiner – möglicherweise unvollständigen – Untersuchung der AGB und Vertragsformulare einer Reihe von Zugangs-Providern ist enttäuschend:

Einigen ist der Datenschutz nicht einmal eine Erwähnung wert. Andere reduzieren ihre Unterrichtung auf allgemeine Floskeln unter der zunächst vielversprechenden Überschrift „Geheimhaltung und Datenschutz“. Mehrere Zugangs-Provider, deren AGB bzw. Vertragsformulare nicht online verfügbar sind, habe ich per E-Mail gebeten, mir entsprechendes Informationsmaterial zukommen zu lassen. Obwohl auf den jeweiligen Homepages eine umgehende Bearbeitung jeglicher Anfragen zugesichert wird, bleiben diese Provider mir nach vier Monaten (bei Redaktionsschluß) noch eine Antwort schuldig, so daß ich auch darüber nichts Erfreuliches berichten kann.

Die Anbieter von anderen Telediensten, z. B. Online Shopping, „glänzen“ fast alle durch Unterlassen der erforderlichen Hinweise, allenfalls findet sich im Kleingedruckten, daß die personenbezogenen Daten vertraulich behandelt werden.

Mit Einwilligung des Nutzers erlaubt das TDDSG auch eine Verwendung der personenbezogenen Daten über den gesetzlichen Rahmen hinaus. Eine solche Verwendung „zu anderen Zwecken“ liegt meistens im Bereich der Werbung und Marktforschung, aber auch im Adressenhandel. Auch hier ergab meine Untersuchung ein ähnlich enttäuschendes Bild.

Wenn überhaupt etwas dazu gesagt wird, findet es sich – als Kleingedrucktes versteckt – in den AGB und auch mal im Vertragsformular selbst. Einige Beispiele sollen die Mängel belegen:

- Der Provider teilt mit, daß er *„bestimmte Daten des Kunden“* an Dritte weiterleitet, *„insoweit es im Rahmen der Anwendung internationaler Datennetze üblich oder vorgegeben oder technisch notwendig ist.“*
- Der Nutzer willigt durch Unterzeichnung des Vertrags in die Verarbeitung und Nutzung seiner Daten ein, *„soweit dies für Zwecke der Werbung, Kundenberatung oder Marktforschung erforderlich ist.“*
- *„Soweit nicht durch die Übermittlung offenkundige Interessen des Teilnehmers verletzt werden“*, erklärt sich der Nutzer mit der Übermittlung seiner Daten an Dritte automatisch einverstanden.
- Dem Nutzer wird eine Widerspruchsfrist von einem Monat eingeräumt, *„ansonsten gilt sein Einverständnis als erteilt.“*

Diese und ähnliche „Einwilligungserklärungen“ sind weder optisch hervorgehoben, noch findet man eine klare Beschreibung der anderen Verwendungszwecke. Auf das Widerrufsrecht wird nur sehr selten hingewiesen. Unabhängig davon, daß die Provider die präzisen Vorschriften des TDDSG nicht umsetzen, drängt sich somit der Verdacht auf, daß einige sich die Einwilligung erschleichen wollen, in der Hoffnung, daß das Kleingedruckte nicht gelesen wird.

Bei einem Zugangs-Provider muß ein potentieller Nutzer die Teilnahmebedingungen, die „Ethik-Richtlinie“, den Teilnehmerantrag und den zu unterzeichnenden Antragsvordruck genau studieren, um zu erkennen, daß der Anbieter den Zugang zum Internet nur ermöglicht, wenn der Nutzer in eine Übermittlung der Nutzerdaten an Dritte einwilligt. Obwohl eine solche Koppelung zulässig ist, bleiben hier im Gewirr verschiedener Aussagen für den Nutzer zu viele Fragen offen. Der Provider hat schon im Februar 1998 eine Überarbeitung seiner AGB und Anträge angekündigt, nach zehn Monaten ist jedoch immer noch alles beim alten.

Angesichts der geschilderten Fakten scheint mir, daß viele der Internet Provider das Inkrafttreten des Informations- und Kommunikationsdienste-Gesetzes (IuKDG) – und somit des TDDSG – am 1. August 1997 regelrecht verschlafen haben. Leider sieht das Gesetz – im Gegensatz zum Mediendienste-Staatsvertrag der Länder – keine Sanktionsmöglichkeiten vor; dies mag mit ein Grund für den beklagenswerten Status quo sein. Erste beratende Maßnahmen von seiten der Aufsichtsbehörden, die die Diensteanbieter bei der Umsetzung der gesetzlichen Vorschriften unterstützen und die dankbar angenommen werden, lassen hoffen. Im Zuge der Umsetzung der EG-Datenschutz-Richtlinie (95/46/EG) werden möglicherweise auch die Eingriffskompetenzen der Aufsichtsbehörden so erweitert, daß sie stärker als bisher auf das Befolgen der Datenschutzvorschriften hinwirken können (s. o. Nr. 2.1.2).

Daß es auch anders geht, belegen zwei Ausnahmen. Ein Provider gibt in seiner Mitgliedsvereinbarung die Einwilligung des Nutzers vor, wobei er eingehend darstellt, für welche anderen Zwecke er welche Daten seines Kunden nutzt oder weiterleitet. Er erklärt in einem Hinweis zum entsprechenden Paragraphen der Vereinbarung, daß er auf Druck einiger seiner Kunden eine Option in das Anmeldeverfahren aufgenommen hat, die es dem Kunden ermöglicht, die Einwilligung zur kommerziellen Nutzung seiner Daten zu versagen oder auch zu einem späteren Zeitpunkt zu widerrufen. Gleichzeitig kündigt er eine entsprechend überarbeitete Mitgliedsvereinbarung an. Ein künftiger Provider hat sich Rat suchend an mich gewandt, um dem Anspruch an eine gesetzeskonforme Gestaltung seines Dienstes von vornherein gerecht zu werden.

Daß dies keine Einzelfälle bleiben müssen, zeigen die Bemühungen, gemeinsam mehr Datenschutz in den Telediensten zu erreichen (s. u. Nr. 8.2.2).

8.2.2 Es geht nur mit Datenschutz!

Die im Vorkapitel beschriebenen Mängel bei Telediensten stehen im direkten Gegensatz zu der Erkenntnis auch und gerade vieler Anbieter, daß wirksame Garantien für die Privatsphäre der Nutzer eine wesentliche Voraussetzung für das erhoffte Wachstum dieses neuen Marktes sind. Es dürfte deshalb nur eine Frage der Zeit sein, daß Datenschutz wenigstens im gesetzlich geforderten Umfang zum selbstverständlichen Inhalt der Teledienstleistungen wird. Maßgebliche Impulse dazu haben die Beteiligten selbst gegeben.

Deutsche Datenschutzexperten aus Kreisen der Wirtschaft, der Gewerkschaften, der Verbraucher, von Fachverbänden, der Wissenschaft und der staatlichen Regulierungs- und Aufsichtsbehörden haben in einem Arbeitskreis unter Federführung des Datenschutzbeauftragten eines großen Anbieters Datenschutz-Standards für Multimedia-Dienstleistungen in Form von Prinzipien und Leitlinien erarbeitet. Sie stellen eine geeignete Grundlage für die Entwicklung konkreter Datenschutzkonzepte dar, deren Umsetzung im Rahmen einer internen oder externen Auditierung durch einen Soll-Ist-Vergleich überprüft und bestätigt werden kann. Diese Initiative zeigt, daß ein Datenschutz-Audit – trotz Streichung aus dem Gesetzentwurf des TDDSG (vgl. 16. TB Nr. 8.1; s. aber die jüngsten Vorschläge des BMI im Rahmen der Diskussion um die Novellierung des BDSG oben Nr. 2.1.2) – von vielen als ein adäquates Mittel zur Durchsetzung des Datenschutzes angesehen wird. Das Entwurfspapier steht seit Januar 1999 der Öffentlichkeit zur Diskussion und Kommentierung – u. a. im Internet unter www.gdd.de – zur Verfügung.

Die Selbstregulierung in Form einer freiwilligen Auditierung wird auch im Schlußbericht der Enquete-Kommission „Zukunft der Medien in Wirtschaft und Gesellschaft – Deutschlands Weg in die Informationsgesellschaft“ vom Juni 1998 (Drucksache 13/11004) angeregt. Im Rahmen der Evaluierung des IuKDG bemüht sich das BMWi, Vorschläge für entsprechende gesetzliche Rahmenbedingungen zu erarbeiten, wobei auch die Ergebnisse der o. a. Arbeitsgruppe berücksichtigt werden sollen.

International und damit für alle Nutzer der WWW-Technik im Internet arbeitet das World Wide Web Consortium, eine weltweite Vereinigung mehrerer hundert Wirtschaftsorganisationen, an dem „Platform for Privacy Preferences“-Projekt (P3P). Damit soll dem Nutzer die Möglichkeit geboten werden, seine Anforderungen an den Schutz der eigenen Daten so in seiner Navigationssoftware zu verankern, daß er (ungefragt) nur mit Anbietern in Kontakt kommt, die den von ihm gewünschten Datenschutz bieten. Obwohl die unterschiedlichen Gesetzeslagen und auch Interessen bei der Festlegung des technischen Standards einige Probleme aufwerfen und der Entwurf aus europäischer Sicht einige Defizite aufweist, halte ich diese Initiative für einen wichtigen Schritt in die richtige Richtung. Denn derart abgestimmte Regelungen ermöglichen dem Nutzer trotz der unterschiedlichen Bedingungen, die aus der Globalität des Internet erwachsen, den Schutz seiner Daten mit leicht einsetzbaren Mitteln selbst zu bestimmen.

Einen ähnlichen Ansatz verfolgt auch TRUSTe, eine von US-amerikanischen Firmen ins Leben gerufene Non-Profit-Organisation, mit ihrem TRUSTe-Konzept:

Nach einer entsprechenden Überprüfung erhalten Anbieter ein „Datenschutzsiegel“ zur Verwendung auf ihrer Homepage. Dadurch kann der Nutzer bei der Kontaktaufnahme erkennen, ob und in welchem Ausmaß ein Anbieter datenschutzrechtliche Grundsätze beim Umgang mit Nutzerdaten respektiert.

8.2.3 Scheitert der elektronische Handel am Geld?

Mit der steigenden Zahl der Internet-Nutzer erhofft sich die Wirtschaft ein explosives Wachstum im Electronic Commerce. Entsprechend wird das Angebot an Waren (z. B. Bücher, Lebensmittel, EDV-Produkte) und Dienstleistungen (z. B. Reisebuchungen, Börsengeschäfte) im Internet ständig erweitert. Solange die Nutzer in den virtuellen Märkten jedoch die Verletzung ihrer Privatsphäre und den Mißbrauch ihrer Daten fürchten müssen, werden diese Angebote nicht im gewünschten Maße in Anspruch genommen. Daher können nur vertrauensbildende Maßnahmen, insbesondere der Einsatz von sicherer und datenschutzfreundlicher Technik und Transparenz bei der Verarbeitung von personenbezogenen Daten, die Akzeptanz der neuen Medien als globaler Handelsraum erhöhen und langfristig sichern.

Das gilt sowohl für das Liefern der Waren oder Dienstleistungen als auch für das Bezahlen im Netz. Anders als beim klassischen – anonymen – Einkauf fallen bei den derzeit im Netz verwendeten Zahlungsverfahren (Nachnahme, Lastschrift, Kreditkartenzahlung) personenbezogene Daten an, die durch den Einsatz der neuen Techniken in einem früher nicht erreichbaren Umfang gesammelt und zu Kundenprofilen verdichtet werden können. Darüber hinaus sind gerade die Bankdaten anfällig für Mißbrauch, nicht nur auf ihrem Weg durch das Netz, sondern auch, weil ihre Sammlung bei der Bank des Kunden dort eine Analyse seines Konsumverhaltens ermöglicht. Deshalb fordert § 4 Abs. 1 TDDSG die Diensteanbieter auf, den Nutzern die *„Bezahlung anonym oder unter Pseudonym zu ermöglichen, soweit dies technisch möglich und zumutbar ist.“*

Es wurden zahlreiche unterschiedliche Zahlungssysteme entwickelt, die den gleichermaßen hohen Anforderungen an Manipulationssicherheit und Datenschutz Rechnung tragen wollen. Einige von ihnen werden derzeit in geschlossenen Gruppen interessierter Teilnehmer (Bank, Händler, Kunden) erprobt.

Das Zahlungssystem *Ecash* der Firma DigiCash, mit dem die Deutsche Bank im Herbst 1997 mit mehreren angeschlossenen Händlern und über tausend Kunden ein Pilotprojekt begonnen hat, ist ein bargeldorientiertes Verfahren, bei dem der Kunde beim Zahlungsvorgang gegenüber der Bank und dem Händler anonym bleibt (s. u. Nr. 8.3).

Neben diesem anonymen Zahlungssystem gibt es kreditkartengestützte Zahlungsverfahren, die ein pseudonymes Bezahlen gegenüber dem Händler ermöglichen. Der Kunde gibt beim Händler seine Kreditkartennummer verschlüsselt an. So kennt der Händler nur die Ware, den Kreditkartentyp und den Kaufbetrag, nicht aber den Kunden; und die Kreditkartengesellschaft kennt den Kunden, den Betrag und den Händler, nicht aber die Ware. Durch Einschalten eines Treuhänders als Vermittler zwischen Händler und Kreditkartengesellschaft ist es zusätzlich möglich, dieser auch den Händler zu verbergen.

Beide Systeme ermöglichen anonymes Bezahlen im Netz, wobei dies für kreditkartengestützte Systeme ohne Treuhänder nur bedingt gilt, da hier die Kreditkartengesellschaft personenbezogene Teilprofile erstellen könnte. Welches System sich schließlich auf dem Internet-Markt durchsetzten wird, bleibt abzuwarten. Möglicherweise laufen intelligente Chipkartensysteme, soweit sie sich zum anonymen Bezahlen in internationalen Datennetzen eignen, den dargestellten Systemen mittelfristig den Rang ab.

Eine ganz andere Art des „Bezahlens“ bietet die *New York Times* an:

Gegen die Angabe von personenbezogenen Daten, deren Umfang weit über das für eine elektronische Versendung erforderliche Maß hinausgeht und die auch zu Werbezwecken an Dritte übermittelt werden, kann der interessierte Leser die Zeitung kostenlos beziehen. So interessant dieses Modell auch deshalb ist, weil die – hier geldwerten – Daten nicht unbedingt die Wahrheit wiedergeben müssen, sein Anwendungsbereich wird im Verhältnis zum erhofften Umfang des elektronischen Handels gering bleiben.

8.2.4 „Versteckte Kamera“ im Internet

„Data Mining heißt das Zauberwort“, sagt die Werbung und preist damit ein Verfahren, um aus sehr großen Datenbeständen Zusammenhänge hervorholen zu können, die bislang nicht bekannt waren. Der Einsatz von Methoden der künstlichen Intelligenz ist hierbei wohl noch eher Zukunftsmusik, doch auch mit konventionellen Datenbanktechniken lassen sich schon gut verwertbare Ergebnisse erzielen. Die verknüpften Informationen werden ausgewertet und gewonnene Erkenntnisse für Planungen und Entscheidungen genutzt:

Unternehmen können ihr Angebot kundenorientiert gestalten und ihre Kunden durch Direkt-Marketing zielgerichtet ansprechen. Sie können aber auch die Beziehungen zu solchen Kunden abbrechen, deren Datenprofil keine Gewinne erwarten läßt. Unabhängig von den sicherlich berechtigten Geschäftsinteressen der Unternehmen zeigt sich hier ein Trend, der aus datenschutzrechtlicher Sicht problematisch ist und angesichts weltweiter Datennetze eine neue Dimension erhält.

Die Voraussetzung für Data Mining (wörtlich „Daten-Bergbau“) ist das Vorhandensein möglichst vieler Daten und Informationen über viele einzelne Kunden. Und so wird oft in der ergiebigsten und billigsten Quelle – dem Internet – alles gesammelt, was anfällt.

Jeder Schritt, jeder Zugriff des Nutzers auf eine Website wird von den Servern protokolliert, wobei die Internet-Adresse zunächst noch keine Rückschlüsse auf die Identität des Nutzers zuläßt. Aber „Cookies“ oder Registrierungen durch einen Nutzernamen und ein zugehöriges Paßwort ermöglichen es, ihn beim nächsten Besuch als „alten Bekannten“ zu erkennen und die schon gesam-

melten Daten zu ergänzen. Einen Schritt weiter gehen Websites, die ihre Nutzer nach persönlichen Daten und Interessen fragen, die dann vielleicht angesichts der dafür angebotenen Vorteile bereitwillig preisgegeben werden. Und spätestens wenn der Nutzer bei einer Online-Bestellung seine Lieferanschrift nennt, macht er sich im Netz auch persönlich bekannt.

Als wahre Fundgruben für Datensammler erweisen sich auch Suchmaschinen, News Groups („Schwarze Bretter") und Chat Rooms („Plauderräume"), denn hier lassen sich Interessen und Meinungen ablesen und zu einem Profil zusammenführen. Spezielle Programme – deren Einsatz in einem ausländischen Server nicht unbedingt rechtswidrig ist – durchsuchen E-Mails nach Inhalten, um Informationen über den Absender zu erhalten. Und mit jeder Äußerung zu einem beliebigen Thema liefert der Internet-Nutzer ein weiteres Mosaiksteinchen zu seinem Persönlichkeitsprofil.

Solange das Sammeln von Daten ohne Bezug zu einer bestimmten Person oder unter einem Pseudonym erfolgt, mag der Nutzer sich noch in Sicherheit wiegen. Doch sobald seine Identität bekannt ist, unterliegen alle seine damit verknüpfbaren Daten Mechanismen, die er nicht mehr kontrollieren kann.

Hat er also seine Daten – mit oder ohne Kenntnis der vielfältigen Auswertungsmöglichkeiten – erst einmal in die Welt des Internet geliefert, so können sie fern jeder Zweckbindung und ohne sein Wissen nicht nur gesammelt, sondern auch weiterverkauft werden, und er weiß nicht, wer welche Daten über ihn woher hat. Unter diesen Umständen erhöht der Einsatz von Data Mining die Gefährdung des Persönlichkeitsrechts des Nutzers. Denn sein auf diese Weise aus den gesammelten Daten zu Tage gefördertes Profil der Interessen oder Neigungen kann falsch oder richtig sein; aber kaum einem wird es recht sein, daß es hinter seinem Rücken frei verfügbar ist.

Da sich das Internet aufgrund seiner Globalität einer wirksamen Kontrolle offensichtlich entzieht, muß der Nutzer selbst für seinen Schutz sorgen. Das TDDSG hat durch die Forderung, eine anonyme oder pseudonyme Nutzung des Internet zu ermöglichen, eine entsprechende Basis geschaffen. Es liegt an jedem einzelnen selbst, ob er die Angebote zum Schutz seiner Daten auch nutzt (s. auch Nr. 8.4).

8.3 Exkurs: Das Prinzip der digitalen Münze

Daten, die einen Geldwert so repräsentieren, daß sie sich zum anonymen Bezahlen in Datennetzen eignen, werden im fachlichen Sprachgebrauch „digitale Münzen" genannt. In dieser Kurzdarstellung wird im weiteren nur *„Münzen"* als Ausdruck verwendet, obwohl diesen *Münzen* einige wesentliche Eigenschaften der anfaßbaren Münzen fehlen – z. B. die, daß es in der Regel mehrere identische Münzen gibt – und digitale Münzen deshalb eher Schecks ähnlich sind.

8.3.1 Gelöste Probleme

Ein Verfahren zur Herstellung und Verwendung von *Münzen* für Zwecke des anonymen Bezahlens in Datennetzen muß u. a. folgende Schwierigkeiten überwinden:

- Die *Münzen* müssen ihren Nennbetrag wert sein. Das wird insbesondere dadurch erreicht, daß eine Bank beteiligt ist, die garantiert, demjenigen den Gegenwert zu erstatten, der ihr die von ihr herausgegebene *Münze* präsentiert.
- Die *Münzen* müssen „bezahlt" bzw. der Betrag der präsentierten *Münzen* muß „ausgezahlt" werden. Zu diesem Zweck richtet die Bank für alle Teilnehmer am Verfahren – Kunden und Akzeptanten – spezielle Konten ein, über die die Transaktionen in Form von Buchgeld abgewickelt werden.
- Eine *Münze* darf – obwohl sie aus Daten besteht, die man leicht kopieren kann – nicht dupliziert und mehrfach erfolgreich zur Gutschrift präsentiert werden können. Deshalb wird die *Münze* bei der Speicherung auf dem Kunden-PC und bei der Übertragung verschlüsselt. Zusätzlich führt die beteiligte Bank eine Liste der bereits eingelösten *Münzen* und beschränkt ihre Garantie auf das erste Präsentieren.
- Es dürfen – anders als bei normalen Münzen – nicht (zufällig) mehrere identische *Münzen* korrekt in Umlauf gebracht werden. Deshalb enthält jede *Münze* eine Identifikationsnummer (im folgenden „Münznummer"), die aus fast 50 Ziffern besteht und jeweils zufällig gewählt wird. Die Möglichkeiten, solche Nummern zu wählen, sind so zahlreich, daß eine zufällig wiederholte Wahl derselben Zahl praktisch ausgeschlossen ist.
- Man muß einer *Münze* am PC „ansehen" können, daß (ob) sie echt ist. Das wird durch eine digitale Signatur der Bank erreicht (s. dazu z. B. 16. TB Nr. 8.1.1).
- Die *Münze* muß einen bestimmten Wert darstellen. Dazu ist jedem der möglichen Werte, die von der Bank vorgegeben sind (z. B. für die Werte von 2^0 bis 2^{15} Pf, also 1 Pf, 2 Pf, 4 Pf, 8 Pf bis zu 327,68 DM), ein bestimmtes Signatur-Schlüsselpaar (aus geheimem und öffentlichem Schlüssel) zugeordnet, dessen Bestandteile während des Herstellungs–, Signatur– und Überprüfungsvorgangs der *Münze* in den technischen Verfahren eingesetzt werden (müssen), so daß der Wert immer eindeutig festgelegt ist. Durch dieses Schlüsselpaar ist auch die Identität der Bank, die Währung und die Gültigkeitsdauer der Münze bestimmt.
- Wenn der Bank eine *Münze* von einem Akzeptanten zur Gutschrift präsentiert wird, soll die Bank nicht erkennen können, welchem Kunden sie diese *Münze* ausgestellt hat. Deshalb wählt der Kunde die Münznummer und die Bank signiert „blind" (s. u.).

8.3.2 Wesentliche Verfahrensschritte

Die Darstellung orientiert sich an dem Verfahren Ecash, wobei Auswahl-, Berechnungs- und Kryptoverfahren nicht beschrieben werden. Auch nicht extra erwähnt wird, daß alle übermittelten Nachrichten zur Sicherstellung der Vertraulichkeit der Daten und Transaktionen verschlüsselt und zum Nachweis der Authentizität der Teilnehmer signiert werden und daß jeder Empfänger signierter Daten die Gültigkeit der Signatur prüft. Diese

Verfahren sind zum Teil recht kompliziert, werden aber von den beteiligten Computern, die jeweils ihre Benutzer „vertreten“, so schnell erledigt, daß diese damit nicht belastet werden. Deshalb stört es auch nicht, daß z. B. die Signatur der Bank länger ist als die Münznummer. Vernachlässigt wird ebenfalls, daß bei einem Herstellungsvorgang im allgemeinen nicht nur eine, sondern mehrere *Münzen* erzeugt werden, die den gewünschten Gesamtbetrag ergeben.

Der Lebenslauf einer *Münze* besteht im wesentlichen aus den folgenden Ereignissen:

– Der Kunde, der eine *Münze* bekommen möchte, wählt zunächst eine als Münznummer geeignete Zahl (s. o.). Damit die Bank beim Signieren die Münznummer nicht erkennt, multipliziert er diese Nummer mit einem sog. Blendungsfaktor, den die Bank nicht kennt und der so gebildet ist, daß der Kunde den Effekt, der von diesem Faktor auf die Signatur der Bank wirkt, später herausrechnen kann. Die so verdeckte Münznummer sendet er mit seiner Kontonummer und der Angabe des gewünschten Betrages an die Bank.

– Die Bank prüft die Daten und bucht den Betrag vom Konto des Kunden ab. Sie wählt unter ihren Signaturschlüsseln denjenigen aus, der dem Betrag entspricht, signiert damit die verdeckte Münznummer und schickt die betragsgerecht signierten Daten an den Kunden.

– Der Kunde rechnet den Blendungsfaktor heraus, d. h. er rechnet die Signatur der verdeckten Münznummer in die Signatur der Münznummer um, und speichert zur späteren Verwendung die Daten seiner nun gültigen *Münze*, die aus der (einmaligen) Münznummer, der betragsgerechten Signatur der Bank und dem Wert der Münze besteht. Die Bank weiß nicht, welchem Kunden sie zu dieser *Münze* verholfen hat, denn bei der Einlösung der *Münze* kann sie an der Signatur zwar erkennen, daß die Signatur von ihr stammt, sie hat die Münznummer (und diese Signatur) wegen des Blendungsfaktors aber nicht gesehen, sondern sie hat „blind“ signiert.

– Beim Bezahlen sendet der Kunde die *Münze* (oder je nach Betrag mehrere) an den Akzeptanten. Wenn der Akzeptant die *Münze* dann zur Gutschrift einreicht, prüft die Bank, ob die *Münze* „echt“ ist und ob sie nicht schon eingelöst wurde (s. o.). Nach der Gutschrift registriert die Bank die Münznummer, um sich in Zukunft dagegen schützen zu können, daß sie dieselbe *Münze* noch einmal einlöst.

8.3.3 Randfragen

– Die Gültigkeit der *Münzen* ist auf einen bestimmten Zeitraum (in der Regel einige Monate) beschränkt, da in periodischen Abständen neue Signatur-Schlüsselpaare erzeugt und verwendet werden. Dadurch wird die Größe der von der Bank geführten Liste der eingelösten *Münzen* begrenzt und mögliche Angriffe auf die geheimen Signaturschlüssel erschwert. Alle „alten“ *Münzen*, d. h. *Münzen* mit nicht mehr gültiger Signatur, kann der Kunde nur noch direkt bei der Bank einlösen. Er kann natürlich auch gültige *Münzen* durch die Bank einlösen lassen und unterscheidet sich insoweit nicht wesentlich von einem Akzeptanten.

– Damit sichergestellt ist, daß nur ein berechtigter Akzeptant – z. B. ein Händler, mit dem der Kunde den Kauf einer Ware vereinbart hat – die Gutschrift für die eingesetzten *Münzen* erhält, wird durch bestimmte technische Verfahrensschritte die Zahlung an den Akzeptanten „gekoppelt“. Die Bank überprüft vor der Gutschrift seine Berechtigung.

– *Münzen*, die z. B. durch einen Hardware-Fehler des Kunden-PCs verlorengegangen sind, können innerhalb eines festgelegten Zeitabschnitts mit Hilfe eines speziellen Programms wiederhergestellt werden. Die Bank löst danach die noch nicht verwendeten *Münzen* ein. Da sie aber anhand ihrer Liste der schon eingelösten *Münzen* überprüfen muß, welche der wiederhergestellten *Münzen* noch nicht verwendet wurden, erfährt sie auch, welche *Münzen* der Kunde zum Bezahlen eingesetzt hat. Die Anonymität geht somit – für diese Zahlungsvorgänge – verloren.

Das Zahlungssystem Ecash hat das Problem des sicheren und anonymen Bezahlens in Datennetzen durch die geschickte Anwendung von Kryptoverfahren im Prinzip gelöst. Doch obwohl es über eine benutzerfreundliche Oberfläche verfügt und der Computer und die eingesetzten Programme den Benutzer weitgehend entlasten, ist es für den Nicht-Fachmann schwer durchschaubar und kompliziert. Es bleibt abzuwarten, ob es sich am Markt durchsetzen wird.

8.4 Jeder ist sein eigener Datenschützer!

Da innerstaatliche gesetzliche Regelungen nur begrenzt gültig und international abgestimmte Vorschriften zumindest kurzfristig nicht erreichbar sind, stellen Initiativen zur freiwilligen Selbstkontrolle und -regulierung der Anbieter eine notwendige Ergänzung für die Gewährleistung des Datenschutzes in globalen Datennetzen dar. Voraussetzung für ihre Wirksamkeit ist aber, daß sie international fest verankert und dadurch vertrauensbildend sind, daß sie für die Beteiligten Verbindlichkeiten schaffen. Doch mit solchen Regelungen und Maßnahmen ist die Internet-Welt für den Nutzer noch keineswegs in Ordnung. Er erhält damit zwar die Wahl und kann sich mit Sorglosigkeit oder mit „Es-wird-schon-gutgehen“-Einstellung im Internet bewegen – solange es tatsächlich gutgeht. Aber wenn er angesichts der gegenläufigen Interessen vieler Anbieter die Kontrolle über die Preisgabe seiner persönlichen Daten behalten will, muß er den Schutz seiner Daten selbst in die Hand nehmen, d. h. er muß die vorhandenen Angebote zum Schutz seiner Privatsphäre auch annehmen und einsetzen, womit er zugleich Anreize zur Verbesserung und Verstärkung des Angebots gibt.

Wenn auch diese Angebote derzeit noch spärlich sind, so sind sie deshalb aber nicht weniger wirksam:

– Verschlüsselungsprodukte ermöglichen das vertrauliche Versenden von E-Mails.

– Mit Anonymisierungsdiensten für E-Mails und unbeobachtetes „Surfen“ lassen sich die Datenspuren verwischen, die jede Aktion im Internet hinterläßt.

– Und das SSL-Protokoll (**S**ecure **S**ocket **L**ayer), das von jeder neueren Navigationssoftware unterstützt wird, erlaubt eine vertrauliche und integritätssichernde Datenübertragung zwischen Internet-Server und heimischem PC.

Aber unabhängig davon ist das oberste Gebot:

Der Nutzer sollte sich immer genau überlegen, welche persönlichen Daten oder Informationen er im Netz bekannt machen möchte.

Um den Selbstschutz der Internet-Nutzer zu ermöglichen bzw. zu unterstützen und die Bereitschaft zu einem eigenen aktiven Beitrag zum Datenschutz zu fördern, müssen verschiedene Maßnahmen greifen, die auch den Staat als Hüter des Rechts auf informationelle Selbstbestimmung in die Pflicht nehmen. Information und Beratung, die die Risiken bei der Nutzung des Internet bewußt machen und praktische Möglichkeiten zum angemessenen Umgang damit lehren, sind die Grundlage für eine in der multimedialen Welt notwendige Medienkompetenz und geben dem Nutzer die erforderliche Sicherheit, sich im Internet selbstbestimmt bewegen zu können. Einen wesentlichen Beitrag hierzu leistet der Einsatz datenschutzfreundlicher Technik, die durch Datensparsamkeit und für den Nutzer transparenten Umgang mit Daten dessen berechtigte Schutzinteressen umsetzt und dadurch den Weg ins Internet ebnet oder für einige gar erst öffnet. Daher ist es erforderlich, die Entwicklung solcher Technik und entsprechender Infrastruktur gezielt und mit Nachdruck voranzutreiben. Denn auch die Initiativen zur Selbstkontrolle (z. B. Datenschutz-Audit) und Selbstregulierung (z. B. P3P, eTRUST) müssen sonst zwangsläufig ins Leere laufen (s. o. Nr. 8.2.2).

Daß viele Nutzer derweil mit „Verweigerung“ reagieren, mag man an der Tatsache ablesen, daß der elektronische Handel allen positiven Prognosen zum Trotz zumindest in Deutschland nur zögerlich genutzt wird. Einschlägige Befragungen in Übersee nennen datenschutzrechtliche und sicherheitstechnische Defizite als Gründe für die auch dort oft deutlich erkennbare Zurückhaltung, was – zumindest bezogen auf Datennetze – auf ein wachsendes Datenschutzbewußtsein schließen läßt. Solch ein „Druck von unten“ kann einiges bewegen, wie das jüngste Beispiel der Firma Intel zeigt, die als Reaktion auf Proteste und Boykottaufrufe von Datenschützern die Seriennummer ihrer neuen Pentium-III-Prozessoren, die den Rechner und somit auch seinen Benutzer im Netz eindeutig identifizierbar macht, nun standardmäßig gegen das Auslesen sperrt.

8.5 Datenschutzfreundliche Technologien

Die Informationstechnik und hierbei insbesondere die Telekommunikation nimmt mittlerweile in allen Lebensbereichen der Menschen in der modernen Industriegesellschaft eine Stellung ein, wie sie kaum eine andere Technik in den vergangenen Jahren erfahren hat. Ohne moderne Telekommunikation und Computertechnik wäre der westliche Lebensstandard nicht denkbar. In allen Lebensbereichen werden diese Technologien genutzt, sei es beim Telefonieren, Einkaufen oder Reservieren, beim Bestellen unterschiedlichster Produkte und Leistungen (Hotel, Mietwagen, Katalogartikel usw.) oder durch Teilnahme an Online-Diensten sowie am Arbeitsplatz bei der Nutzung eines lokalen oder konzernweiten Netzwerkes. Bei jeder dieser Anwendungen fallen eine Fülle von Einzeldaten über die Benutzer der jeweiligen Dienste an, die detaillierte Aussagen über das Verhalten und die Gewohnheiten jedes einzelnen Nutzers machen und somit ein **Nutzerprofil** bilden.

Den meisten Nutzern ist aufgrund der Komplexität und der mangelnden Transparenz von Systemen der modernen Informations- und Kommunikationstechnik (IuK-Technik) in der Regel nicht bewußt, welche Daten wo, wie lange, zu welchem Zweck und von wem gespeichert werden. Daher rührt die Befürchtung vieler Menschen, mit der Einführung von IuK-Techniken könnte die Privatsphäre des Einzelnen „auf der Strecke“ bleiben.

Viele Betreiber von IuK-Systemen werben deshalb damit, daß der Zugang zu den von ihnen erhobenen, gespeicherten und verarbeiteten Nutzerdaten durch sehr aufwendige technische und organisatorische Sicherheitsmechanismen begrenzt wird. Dies bedeutet aber, daß der Schutz der Privatsphäre lediglich von der Wirksamkeit der üblichen Sicherheitsmechanismen abhängig ist. Daß dies aus datenschutzrechtlicher Sicht äußerst problematisch ist, liegt auf der Hand.

Die Einführung der IuK-Techniken in allen Lebensbereichen und die damit verbundene Diskussion über den Schutz der Privatsphäre haben zu der Erkenntnis geführt, daß die üblichen technischen Schutzmechanismen oft nicht mehr ausreichen. Vielmehr kommt es bereits bei der Entwicklung und Gestaltung von IuK-Systemen auf die Berücksichtigung datenschutzrechtlicher Grundsätze an. Sie werden aus der Sicht des Datenschutzes nur dann den Datenschutzbedürfnissen der Anwender gerecht, wenn sie sich an den Prinzipien der **Datenvermeidung**, zumindest aber an der **Datensparsamkeit**, orientieren. Häufig wird in diesem Zusammenhang dann von datenschutzfreundlichen Technologien, auch „Privacy Enhancing Technology (PET)“ gesprochen.

Die Eckpfeiler moderner IuK-Technik, die in diese Betrachtungen mit einbezogen werden müssen, sind

– klassische Informationstechnik,
– Telekommunikation,
– Multi-Media und
– Chipkarten.

Nur das optimale Zusammenwirken dieser einzelnen Komponenten sichert beispielsweise den dauerhaften Erfolg des Internets. Dies gilt ebenso, wenn es darum geht, datenschutzfreundliche Technologien zu entwickeln und effizient einzusetzen.

Dieser Gedanke findet sich auch in einer Entschließung der 54. Konferenz der Datenschutzbeauftragten des Bundes und der Länder wieder, die die Erforderlichkeit dieser Technik besonders betont und den Gesetzgeber nachdrücklich dazu auffordert, rechtliche Rahmenbedingungen für deren Entwicklung und Einsatz zu schaffen (s. **Anlage 11**).

Um Entwicklern, Anbietern und interessierten Nutzern die Möglichkeiten von datenschutzfreundlichen Tech-

nologien aufzuzeigen, beauftragte die Konferenz der Datenschutzbeauftragten ihren Arbeitskreis „Technische und organisatorische Datenschutzfragen“ damit, einen Leitfaden zu erarbeiten, in dem die wichtigsten technischen Erfordernisse und Rahmenbedingungen für datenschutzfreundliche Technologien aufgeführt sind (s. **Anlage 27**).

Auch die Enquete-Kommission „Zukunft der Medien in Wirtschaft und Gesellschaft – Deutschlands Weg in die Informationsgesellschaft“ des Deutschen Bundestages hat in ihrem Schlußbericht (Drucksache 13/11004) den Einsatz *„datenschutzfreundlicher Technologien (Privacy Enhancing Technology)“* gefordert, um den Schutz des informationellen Selbstbestimmungsrechts in der Informationsgesellschaft aufrechterhalten zu können. Ich hoffe, daß die Forderung in den nächsten Jahren durch die Anbieter und Hersteller aufgegriffen wird und das Recht auf informationelle Selbstbestimmung im Zusammenwirken mit der Technik seine Ausgestaltung findet.

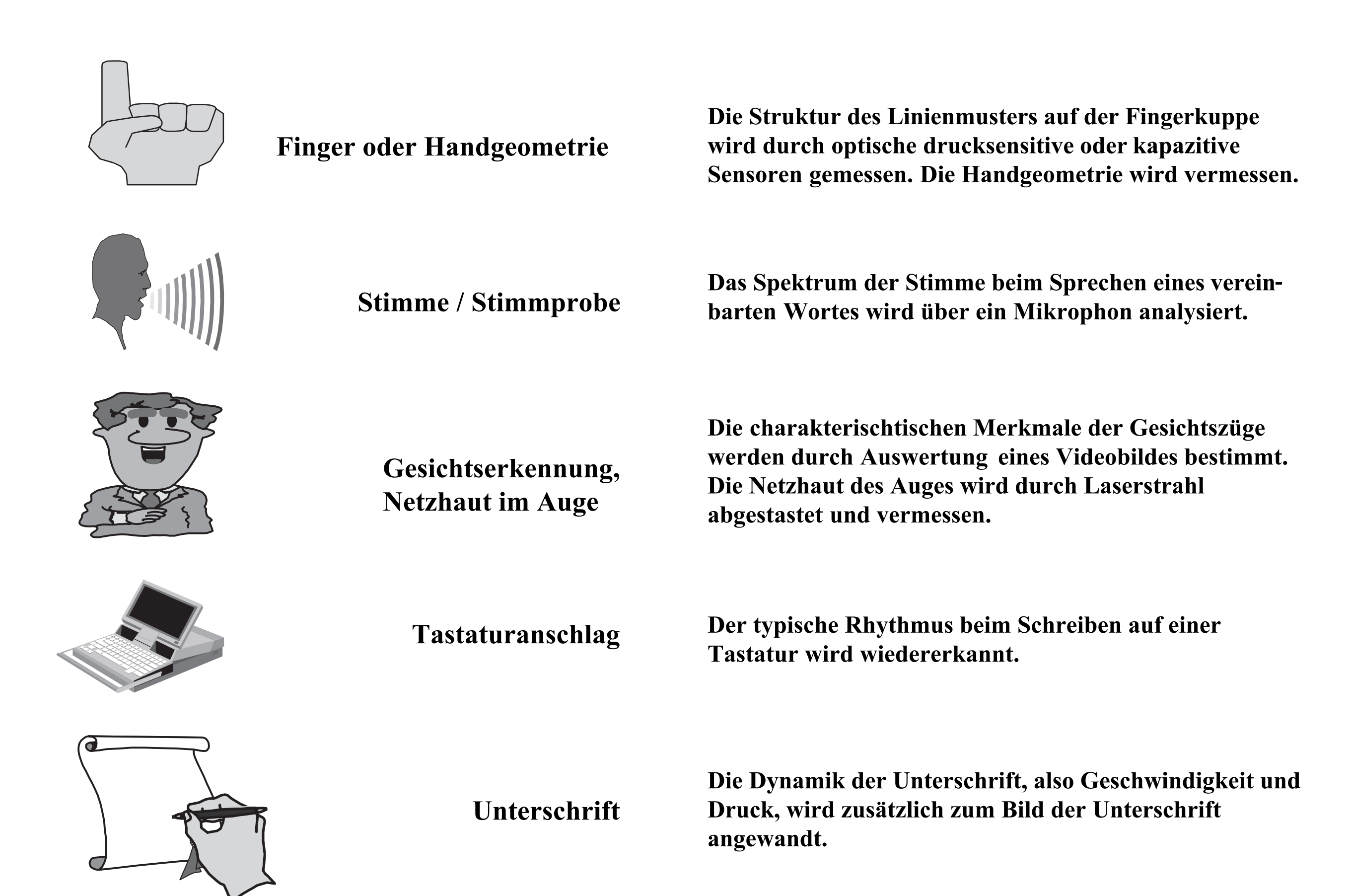
8.6 Biometrische Merkmale: Der Körper als Ausweis?

Wer kennt sie nicht, die Situation nach dem Urlaub: Man steht vor dem Geldautomaten seiner Bank und hat seine PIN vergessen; oder man kommt ins Büro und weiß sein PC-Paßwort nicht mehr. Peinlich wird es auch, wenn das Büro gänzlich verschlossen bleibt, weil man den Zugangscode für das Türschloß nicht mehr weiß. Über die Problematik der Verwendung der vielen Paßwörter, PINs und Zugangscodes habe ich in der Vergangenheit schon ausführlich berichtet (s. 15. TB Nr. 30.1). Seit langem weise ich deshalb auf die Notwendigkeit der Verwendung biometrischer Merkmale hin. Dies muß jetzt auch vertieft datenschutzrechtlich diskutiert werden.

Biometrische Systeme stellen derzeit die einzige Möglichkeit dar, den Zugriffs- oder Zugangsschutz wirksam zu verbessern. Sie beruhen auf unverwechselbaren persönlichen körperlichen Merkmalen, die nicht nur eine sicherere, sondern auch eine anwendungsfreundlichere Zuordnung einer Chipkarte, einer Benutzerkennung oder eines Zugangscodes zu ihrem rechtmäßigen Besitzer ermöglichen als dies bisherige Methoden vermochten. In der Erprobung sind Verfahren, die auf der Auswertung des Fingerabdrucks oder der Handgeometrie, der Stimme, der Gesichtszüge oder der Netzhaut des Auges, des Tastenanschlags beim Schreiben auf einer Tastatur eines PC und der Schreibmotorik bei einer Unterschriftsleistung beruhen (s. Abbildung 4).

Abbildung 4 (zu Nr. 8.6)

Biometrische Identifikationsverfahren



Alle diese Verfahren arbeiten allerdings nach dem gleichen Prinzip:

Zunächst müssen Referenzdaten der Beteiligten erhoben und gespeichert werden, also z. B. die Daten des „echten“ Fingerabdrucks des „echten“ Herrn XYZ. Da im laufenden Betrieb niemals dieselben Bedingungen wie bei der Erhebung der Referenzdaten herrschen, stimmen in den seltensten Fällen die aktuell erfaßten Merkmale und die gespeicherten Referenzdaten vollständig überein. So wird Herr XYZ niemals in absolut gleicher Weise seinen Finger auf das Lesegerät legen; der Druck kann sich ändern, die Hautfeuchtigkeit mag unterschiedlich sein oder die Hauttemperatur schwankt – um nur einige Beispiele für etwaige Einflüsse zu nennen. Deshalb müssen die zulässigen Toleranzen in einem speziellen Auswertealgorithmus, der auf das eingesetzte Verfahren zugeschnitten ist, festgelegt werden. Die Festlegung einer Fehlertoleranz ist deshalb besonders wichtig, weil dadurch die Erkennungsrate – Wieviel gespeicherte „echte“ Benutzer werden als solche erkannt? – des Verfahrens bestimmt wird. Ist die Toleranz zu klein, werden auch berechtigte Benutzer abgewiesen, was sich kritisch auf die Akzeptanz des Systems auswirken kann. Ist sie zu groß, wird hin und wieder ein unberechtigter Benutzer für berechtigt gehalten. Die Zuverlässigkeit des Verfahrens wird dann in Frage gestellt. Das Maß für die Leistungsfähigkeit eines biometrischen Verfahrens ist die Gleichfehlerrate, bei der die Zahl fälschlich abgewiesener und fälschlich akzeptierter Personen gleich groß ist. Praktische Erprobungen beispielsweise des Fingerabdruckverfahrens ergaben eine Gleichfehlerrate im Promillebereich; bei anderen soll sogar die Gleichfehlerrate Null geworden sein.

Aus datenschutzrechtlicher Sicht ist neben dem Problem einer möglichst kleinen Gleichfehlerrate auch noch die Frage von Bedeutung, wo die eigentliche Prüfung der Referenzdaten gegenüber den aktuellen Daten erfolgt:

Etwa lokal auf einer dem Benutzer ausgehändigten Chipkarte oder auf einem eventuell weit entfernt liegenden IT-System bei dem Verfahrensbetreiber. Sicherheitstechnisch gesehen ist eine Prüfung der Daten auf einem lokalen, im Besitz des Nutzers verbleibenden System (Chipkarte mit Sensoren) die optimale Lösung. Nicht nur, daß damit dem Selbstbestimmungsrecht des Nutzers in hohem Maße Genüge getan wird, sondern auf diese Weise können auch Manipulationsversuche, unzulässige Speicherungen oder Zweckänderungen gänzlich ausgeschlossen werden. Am Markt ist dieses Verfahren schon zumindest für das Fingerabdruckverfahren verfügbar. Die Referenzdaten wie auch die aktuellen Daten werden dabei auf einer Chipkarte erhoben, gespeichert und verarbeitet. Bei der Nutzung, z. B. zur Zugangskontrolle, wird die Chipkarte in ein Lesegerät gesteckt und der Finger auf die Chipkarte gedrückt. Von dieser wird der aktuelle Fingerabdruck erfaßt, digitalisiert und dann mit den Referenzdaten aus der Chipkarte verglichen. Das Ergebnis (Akzeptanz oder Abweisung) wird dem Lesegerät bereitgestellt. Damit ist sichergestellt, daß die biometrischen Daten den Verfügungsbereich des Benutzers ohne dessen Einwilligung nicht verlassen und in unberechtigte Hände gelangen können.

Bei anderen Merkmalen scheint eine Integration auf einer Chipkarte nicht möglich, weil das hierzu notwendige Erfassungsgerät zu groß sein dürfte. Ein Beispiel hierfür ist die Verwendung der Gesichtszüge. Denn hier besteht immer die Gefahr, daß auf dem Weg zwischen der Erfassung der aktuellen Daten und dem Vergleich mit den Referenzdaten eine Verfälschung herbeigeführt wird bzw. daß die Daten unzulässigerweise gespeichert oder verarbeitet werden. Die Gesamtsicherheit des Systems hängt damit von der Vertrauenswürdigkeit **aller** für die Verarbeitung der Daten notwendigen Komponenten eines Systems ab. Eine Zertifizierung der Sicherheit nach den europäischen Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik (ITSEC oder Common Criteria) scheint damit unerläßlich. Die Höhe der Zertifizierung, d. h. der anzulegende Maßstab, muß sich dabei an den Anforderungen der Benutzer orientieren; mit Blick auf die Diskussionen beim Signaturgesetz (SigG) sollten Zertifizierungen mindestens im Bereich „ITSEC E3“ und „E4 hoch“ angestrebt werden.

Neben diesen Problemen ist aus datenschutzrechtlicher Sicht ebenfalls zu klären, wie eine **Zweckänderung** der Biometriedaten verhindert werden kann. Verlassen Referenzdaten und aktuelle Daten den Verfügungsbereich des Benutzers, muß sichergestellt werden, daß eine Zweckänderung der Daten ausgeschlossen werden kann. Für das Fingerabdruckverfahren würde dies beispielsweise bedeuten, daß ein Datenabgleich mit dem Bestand des beim BKA geführten Fingerabdruckidentifizierungssystems – AFIS – (siehe auch Nr. 11.8 und u. a. im 15. TB Nr. 23.3) technisch ausgeschlossen werden kann. Hierbei handelt es sich um ein durchaus schwieriges Unterfangen, dessen technische und organisatorische Realisierbarkeit noch nicht abschließend geklärt ist.

Ein Problem haben übrigens alle heutigen biometrischen Verfahren:

Es gibt immer einen gewissen Prozentsatz der Bevölkerung, dem das entsprechende biometrische Merkmal nicht zur Verfügung steht – beispielsweise Personen ohne Arme, ohne Augen oder Menschen, die stumm sind. Wissenschaftler möchten deshalb diese Lücke durch die Einführung eines Erbguttests in Echtzeit (Online-DNA) schließen. Diese Entwicklung bedarf einer intensiven Diskussion, für die eine datenschutzrechtlicher Begleitung unerläßlich ist.

8.7 Die digitale Signatur – endlich Realität?

Über die Möglichkeiten und die Verfahrensweise der digitalen Signatur habe ich bereits im 16. TB (Nr. 8.1.1) berichtet. Das Signaturgesetz (SigG) trat am 1. August 1997 in Kraft. In Verbindung mit der Signaturverordnung (SigV), die am 1. November 1997 in Kraft trat, hat der Gesetzgeber auch die letzte Hürde beseitigt und den rechtlichen Rahmen dafür geschaffen, daß Rechts-

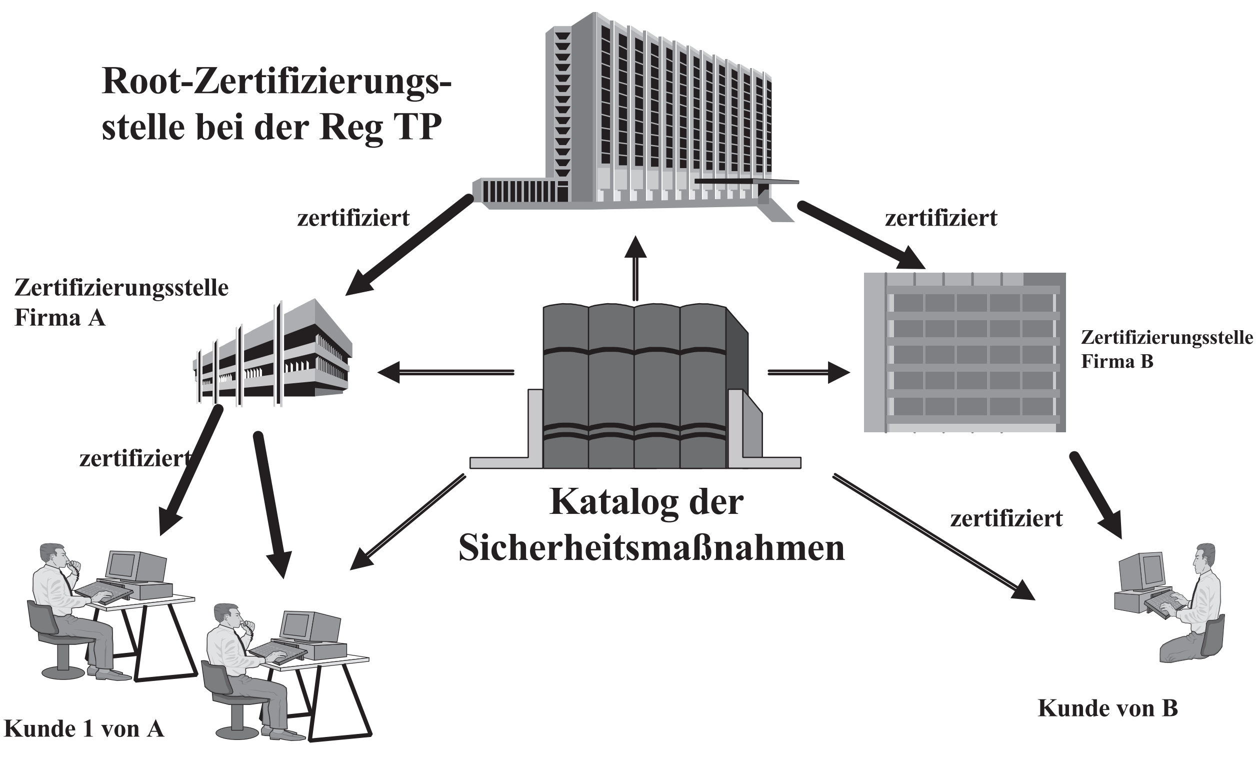
geschäfte über offene Netze, wie das Internet, wirksam und sicher abgeschlossen werden können. Bedauerlicherweise haben Zertifizierungsstellen („Trust Center“) erst ab Anfang 1999 den Betrieb aufnehmen können. Dies liegt zum einen daran, daß die Kataloge von geeigneten Sicherheitsmaßnahmen gemäß § 12 Abs. 2 und § 16 Abs. 6 SigV erst zum 30. Oktober 1998 veröffentlicht wurden, und zum anderen, daß der Betrieb der sogenannten „Root-Zertifizierungsstelle“ bei der Regulierungsbehörde für Telekommunikation und Post (RegTP) ihren Betrieb erst zum 23. September 1998 aufgenommen hat.

Um ein Dokument digital unterschreiben – d. h. signieren – zu können, benötigt der Benutzer zunächst ein auf ihn persönlich ausgestelltes Schlüsselpaar. Dieses besteht aus einem „privaten (geheimen) Schlüssel“ und einem dazugehörenden „öffentlichen Schlüssel“. Der „private (geheime) Schlüssel“ wird dem Benutzer auf einer Chipkarte ausgehändigt, die – vergleichbar der PIN bei der ec- oder Kreditkarte – durch geeignete Sicherheitsmechanismen vor dem Zugriff Unbefugter geschützt sein muß. Der „öffentliche Schlüssel“ wird hingegen in einem jedermann zugänglichen Verzeichnis veröffentlicht. Beide Schlüssel erhält der Benutzer nach Abschluß eines Vertrages gegen Vorlage seines Personalausweises oder vergleichbarer Dokumente von einer Zertifizierungsstelle, dem „Trust-Center“. Damit kommt der Zertifizierungstelle eine zentrale Bedeutung zu. Die Sicherheit und Vertrauenswürdigkeit dieser Stellen sind die notwendigen Voraussetzungen für einen sicheren Betrieb des Verfahrens.

Die Richtigkeit des Signaturschlüssels einer Zertifizierungsstelle wird durch die „digitale Signatur“ der sogenannten „Root-Zertifizierungsstelle“ garantiert. Darum war es so wichtig, daß die Root-Zertifizierungsstelle (siehe Abbildung 5) bei der Regulierungsbehörde für Telekommunikation und Post im September 1998 endlich ihren Betrieb aufnahm.
Probleme bereitete es auch, die Kataloge der Sicherheitsmaßnahmen gemäß § 12 Abs. 2 und § 16 Abs. 6 SigV zusammenzustellen, für die das Bundesamt für Sicherheit in der Informationstechnik – BSI – zuständig ist. Hierzu wurde aus der Wirtschaft die Kritik geäußert, den Katalogen fehle es an Beispielen aus der Praxis. Eine solche kann es jedoch bisher nicht geben. Auch die Gefahr, die Kataloge bzw. die dort aufgeführten Sicherheitsmechanismen könnten als „normativ“ angesehen werden, sind unbegründet. In der SigV ist ausdrücklich festgelegt, daß die Kataloge lediglich empfehlenden Charakter haben. Gleichwohl muß aus Datenschutzsicht die Entwicklung sorgfältig beobachtet werden.

Abbildung 5 (zu Nr. 8.7)

Zertifizierungshierarchie und Kataloge der Sicherheitsmaßnahmen



Ich hoffe, daß die Industrie sehr bald die Initiative ergreift und auf der Basis der digitalen Signatur Anwendungen anbietet, die es dem Nutzer erlauben, sich anonym oder pseudonym – vor allem aber sicher – in den weltweiten IT-Netzen zu bewegen. Nun liegt es an ihr, die längst fälligen sicheren Anwendungen zu entwickeln.

8.8 SPHINX – ein Schritt zu mehr Sicherheit

Eine Folge der Aufteilung der Ministerien mit den Hauptstandorten Berlin und Bonn ist die Einführung des Informationsverbundes Berlin-Bonn (IVBB), über den ich bereits berichtet habe (16. TB Nr. 34.2). Ein Ziel der Nutzung des IVBB in der Bundesverwaltung ist die Verarbeitung und Übertragung „digitaler Dokumente" mit einer Sicherheit, die der der Papierdokumente gleichwertig ist. Parallel zur Gestaltung und Einrichtung des IVBB wird ein weiteres Netz, nämlich das „bundesweite Intranet der Bundesverwaltung (Informationsverbund Bundesverwaltung IVBV)" geschaffen.

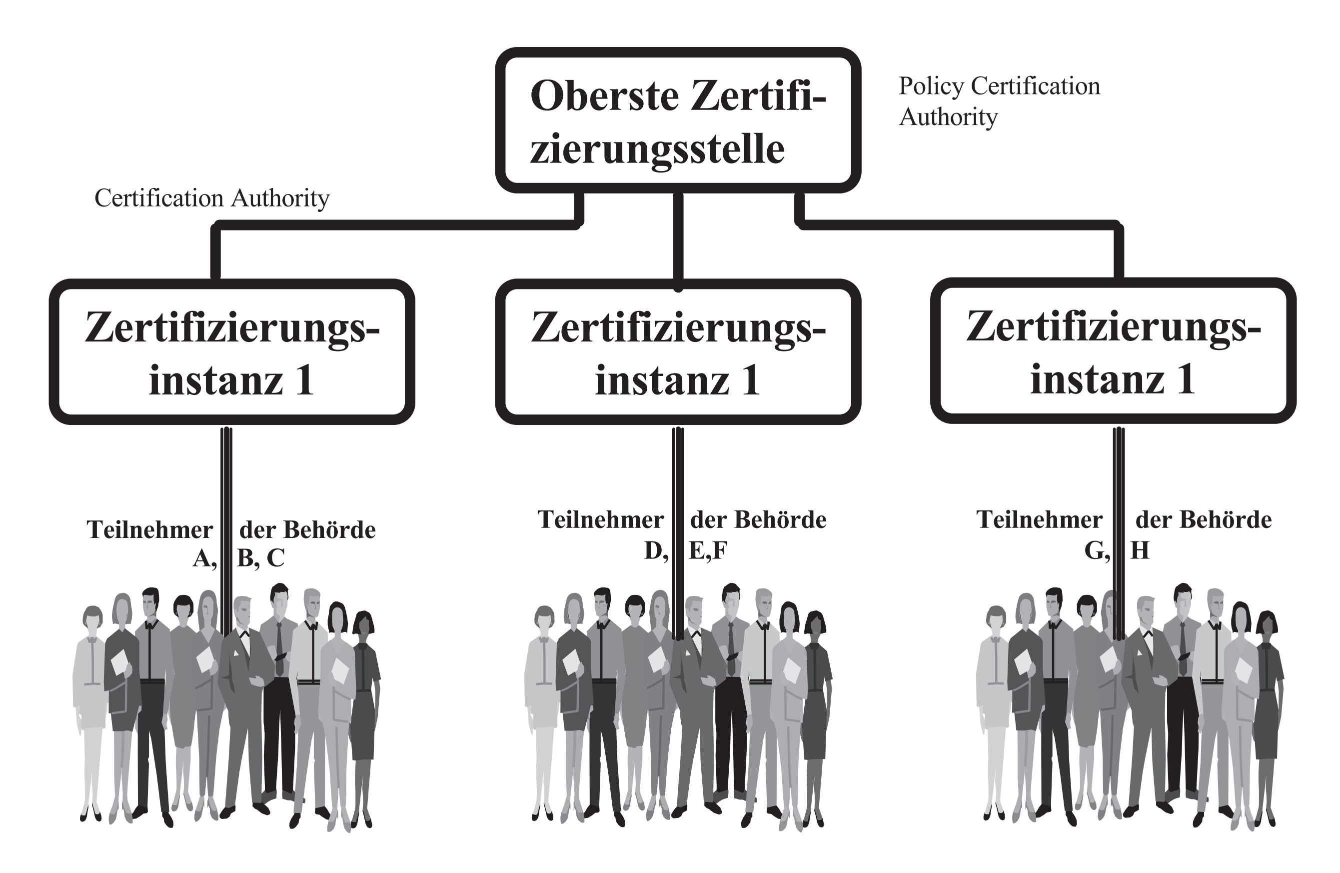
Bei der Verarbeitung digitaler Dokumente in Netzen sind drei Schutzziele zu beachten: Die **Vertraulichkeit** und die **Integrität** der Daten sowie die **Authentizität** des Absenders und Empfängers. Zur Realisierung dieser Anforderungen sind aus technischer Sicht zwei Maßnahmen unerläßlich:

Die **kryptographische Verschlüsselung** der Inhaltsdaten und deren **digitale Signatur**.

Die kryptographische Verschlüsselung der Inhaltsdaten stellt ein geeignetes Instrument zur Sicherung der Vertraulichkeit dar; die digitale Signatur ermöglicht die Kontrolle der Integrität und Authentizität der Daten und der beteiligten Kommunikationspartner. Diese Sicherheitsmaßnahmen müssen vom Absender der Daten bis zum Empfänger wirken.

Solche Verfahren können nur funktionieren, wenn alle Kommunikationspartner technische Verfahren – Hard- und Software – einsetzen, die miteinander verträglich, „interoperabel" sind. Dies gilt besonders für Sicherheitsprodukte, da die Sicherheit nicht an einer Behörden- oder Netzgrenze enden darf. Will man die Sicherheit behördenübergreifend oder länderübergreifend garantieren, sind Standards für die eingesetzten Produkte und deren Herstellerunabhängigkeit gefragt. Zur Vorbereitung der breiten Einführung einer Ende-zu-Ende-Sicherheit im

Abbildung 6 (zu Nr. 8.8)



IVBB und darüber hinaus führt die Koordinierungs- und Beratungsstelle der Bundesregierung für Informationstechnik in der Bundesverwaltung (KBSt) in Zusammenarbeit mit dem BSI den Pilotversuch SPHINX durch. An diesen Versuch beteiligen sich zahlreiche Bundesministerien und nachgeordnete Behörden, aber auch Einrichtungen der Bundesländer. Erprobt werden Sicherheitsprodukte von zehn verschiedenen Firmen. Ziele des Pilotversuches sind

– die Erprobung der Funktionalität und Interoperabilität der Sicherheitsprodukte der beteiligten Firmen,

– die Sammlung von Erfahrungen hinsichtlich der Anwenderakzeptanz sowie

– eine Abschätzung des personellen, finanziellen und organisatorischen Aufwandes.

Um eine weitgehende Herstellerunabhängigkeit zu erzielen, wurden nur Produkte für den Versuch zugelassen, die sich am MailTrusT-Standard des TeleTrust Deutschland e.V. orientieren. Der MailTrust Standard ist ein herstellerübergreifender Standard für digitale Signaturen, der die Aspekte der Interoperabilität und internationale Standards konsequent berücksichtigt und den Anforderungen der relevanten und interessierten Branchen, Verbände und Anwendergruppen entspricht. Seine Verwendung soll eine größtmögliche Interoperabilität garantieren. Ferner soll für die digitale Signatur eine Konformität zum Signaturgesetz angestrebt werden. Beides wird durch die Festschreibung des MailTrusT-Standard garantiert.

Die PC der Pilotversuchsteilnehmer wurden um entsprechende Hard- und Softwareprodukte ergänzt, die das Ver- und Entschlüsseln von Nachrichten sowie das Signieren und Verifizieren von elektronischen Signaturen ermöglichen. Um die Interoperabilität testen zu können, wurden drei Zertifizierungsstellen (Certification Authorities; CA) auf der unteren Hierachieebene und eine übergeordnete Zertifizierungsstelle (Policy Certification Authority (PCA)) eingerichtet (s. Abbildung 6). Die PCA ist das Bindeglied zwischen den drei Zertifizierungsstellen.

Ich begrüße es sehr, daß die KBSt diesen Pilotversuch durchführt und habe den bisherigen Fortgang aufmerksam begleitet, denn ich habe in der Vergangenheit wiederholt die kryptographische Verschlüsselung und digitale Signatur von personenbezogenen Daten bei der Übermittlung über Netze oder auf Datenträgern gefordert. Ich hoffe, daß der Pilotversuch die Realisierbarkeit meiner Forderungen bestätigt und Aufschluß über die erforderlichen Aufwendungen und anstehenden Kosten sowie konkrete Empfehlungen bezüglich der einsetzbaren Produkte und Standards gibt. Darüber hinaus hoffe ich, daß auf der Basis der SPHINX-Ergebnisse eine länder- und behördenübergreifende Sicherheitsinfrastruktur geschaffen wird, die dann Voraussetzung für sichere Anwendungen in offenen Netzen wäre. Das Ende des Pilotversuches wird für Frühjahr 1999 erwartet.

8.9 Hacker und Viren

8.9.1 Hackersoftware und Computerviren für jedermann

„Hacken“ bezeichnet einen Vorgang, der ab und zu in der Öffentlichkeit für Wirbel sorgt, wenn wieder einmal irgendein IT-System durch einen „Hacker“ geknackt wurde. In der Öffentlichkeit entsteht dabei oft der Eindruck, daß ein großes Spezialwissen erforderlich ist, um die Sicherheitsmechanismen zu überwinden. Hierüber würden aber nur wenige Computerbenutzer verfügen, so daß dann der Angriff – wegen seiner vermuteten Seltenheit – verharmlost oder mit Schadenfreude zur Kenntnis genommen wird, weil eine bestimmte Stelle durch den Angriff in der Öffentlichkeit bloßgestellt wurde. Dabei kommt in vielen Berichten zu kurz, daß dies „hacking“ nicht mehr nur von Spezialisten ausgeführt werden kann, sondern auch durch jeden normalen PC-Benutzer, sofern er über die notwendigen Hilfsmittel („Tools“) verfügt. Diese werden vermehrt auf CD-ROM – paradoxerweise z. B. unter dem Titel „Datenschutz-CD“ – vertrieben und im Internet auf einschlägigen Hacker-Seiten kostenlos zur Verfügung gestellt. Gemeinsam ist den mit Phantasie und technischem Verständnis programmierten „Hackerwerkzeugen“, daß sie die Schwachstellen und Sicherheitslücken der eingesetzten Systeme und Programme gezielt ausnutzen. Als typisches Beispiel sei hier auf den Kennwortschutz – gegen das Lesen eines Textes durch andere – in einem weltweit eingesetzten Textverarbeitungssystem verwiesen. In einer älteren Version stand das Kennwort uncodiert an einer definierten Stelle in der Datei und konnte von jedem, der die Stelle kannte, mühelos gelesen werden. In der neueren Version wurde zwar diese Lücke beseitigt, gleichwohl ist mit Kenntnis des Verschlüsselungsalgorithmus ein Berechnen des Kennworts möglich – was durch Hackprogramme auch ausgenutzt wird!

Immer wieder treten deshalb besorgte Bürger an mich heran, die durch die Veröffentlichung solcher Software-Tools und vermutete oder bestehende Sicherheitslöcher die Datensicherheit gefährdet sehen, und bitten mich, gegen die Urheber der Veröffentlichung oder die entsprechenden Firmen vorzugehen.

Für solche Besorgnisse habe ich volles Verständnis. Allerdings habe ich hierbei nur begrenzte Möglichkeiten:

Meine Zuständigkeit beschränkt sich auf die Kontrolle und Beratung von bestimmten datenverarbeitenden Stellen in Fragen des Datenschutzes, also dem Schutz des Persönlichkeitsrechts jedes einzelnen. Allein wegen der Herausgabe einer solchen CD–ROM oder der Veröffentlichung im Internet kann ich nicht tätig werden. Selbst dann, wenn die Anwendung eines auf ihr enthaltenen Programmes (durch einen Käufer der CD-ROM) im Einzelfall zu einer Beeinträchtigung von Persönlichkeitsrechten führen könnte. Erfolgversprechend ist es jedoch, auf die Herstellerfirmen der „geknackten“ Systeme oder Programme einzuwirken und sie zu veranlassen, die von den veröffentlichten „Hackerwerkzeugen“ genutzten Sicherheitslücken oder Schwachstellen schneller und vollständiger als bisher zu schließen. Ich

habe hierzu mit dem Bundesamt für Sicherheit in der Informationstechnik Gespräche zur Einleitung entsprechender Initativen aufgenommen. Meine Anregung wird dort positiv gesehen; über die Art und Weise der Umsetzung ist noch zu entscheiden.

Hiervon unberührt bleibt eine möglicherweise strafrechtliche Relevanz der Herausgabe einer solchen CD-ROM oder einer solchen Veröffentlichung. Dies zu prüfen, ist jedoch Aufgabe der zuständigen Strafverfolgungsbehörden.

Zu berücksichtigen ist daneben, daß die Berichterstattung über Sicherheitsdefizite aber auch positive Wirkungen haben kann. Nach meiner Beobachtung führt das Wissen um Sicherheitslücken oft dazu, daß die Aufmerksamkeit bezüglich der Sicherheit bei verantwortungsvollen Betreibern von Systemen nicht nachläßt. So enthalten zwar die Hacker-Tools Programme und Beschreibungen, die – jedenfalls zum Teil – das unbefugte Eindringen in Systeme oder Dateien ermöglichen. Sie offenbaren dadurch aber auch gleichzeitig Sicherheitslücken. Einzelne Tools enthalten nun Hinweise, wie diese geschlossen werden können. Deren Kenntnis und das Wissen um die Sicherheitslücken ermöglicht es den für die Datensicherheit Verantwortlichen, geeignete Maßnahmen zum Schließen dieser Lücken zu ergreifen.

Die Veröffentlichung von Sicherheitslücken hat auch die Herstellerfirmen in vielen Fällen veranlaßt, Nachbesserungen in ihrer Software oder Hardware vorzunehmen und diese in Form von fehlerfreien binären Programmteilen (Patches), die die Sicherheitslücken beseitigen, ihren Kunden zur Verfügung zu stellen.

Schließlich ist zu bedenken:

Das Nichtveröffentlichen von Sicherheitslücken bedeutet durchaus nicht, daß diese nicht existieren und nicht mißbräuchlich genutzt werden können.

8.9.2 Gefahren aus dem Internet – auch für personenbezogene Daten

Die Nutzung des Internet ist heute für viele selbstverständlich geworden. Weder der Umgang mit der Hardware – PC, Modem usw. – noch mit der wachsend komfortableren, aber auch komplexeren Software bereitet den „Usern“ heute ernsthafte Probleme. Diese scheinbare „Problemlosigkeit“ des Umgangs mit PC und Internet führt allerdings oft zur Sorglosigkeit. Es gerät häufig in Vergessenheit, daß insbesondere das Surfen im Internet Probleme für die Sicherheit des Rechners – insbesondere auch der auf ihm gespeicherten personenbezogenen Daten – mit sich bringt. Da beunruhigen den aufmerksamen Nutzer Nachrichten in der Presse, nach denen es Jugendlichen gelungen ist, Paßworte, die beim Homebanking genutzt werden, aus dem PC auszulesen, was sie in die Lage versetzt hat, Banküberweisungen zu Lasten des Ausgespähten vorzunehmen.

Ganz allgemein wird übereinstimmend festgestellt, daß sich die Sicherheitsprobleme häufen. Ein Ausspionieren aller sich auf dem Rechner befindlichen Daten durch Hacker aus dem Internet ist keine Utopie mehr. So ist es Angreifern nicht nur möglich, ganze Platteninhalte zu lesen und/oder auf einen anderen Rechner zu kopieren, sondern auch die Systemdateien zu verändern. Dadurch kann der PC zum Schaden des ahnungslosen Nutzers mißbraucht werden, z. B. indem Daten verändert, gelöscht oder weitergegeben werden.

Als Ursache für dieses hohe Gefährdungspotential ist vor allem die offene Struktur des Internet mit seiner ständig wachsenden Millionenschar von Nutzern – und potentiellen Hackern – zu sehen. Hinzu kommt der Umstand, daß viele Programme, die die oben beschriebenen Rechnermanipulationen vornehmen können, im Internet selbst frei abrufbar sind (s. o. Nr. 8.9.1)

Sicherheitsprobleme können sich schon einstellen, wenn im Internet Zugriff auf „normale“, statische Informationsseiten – z. B. die eines Buchversandes – genommen wird. Zwar ist dabei normalerweise der Zugriff „von draußen“ auf die im PC gespeicherten Daten nicht möglich. Durch Programmfehler, falsch oder fehlerhaft installierte oder manipulierte Software, Manipulationen oder durch Viren oder andere schädliche Programme ist dies jedoch nie vollständig auszuschließen.

Andere Sicherheitsprobleme können durch falsche Handhabung durch den Benutzer oder durch eine unsachgemäße Konfiguration des Browsers – also des Zugangsprogramms zum Internet – auftreten, aber auch durch Sicherheitslücken im Browser selbst. Das Sicherheitsrisiko wächst, wenn nicht nur statische Seiten aufgerufen, sondern auch Programme aus dem Netz heruntergeladen und auf dem PC ausgeführt werden. Dabei setzt man sich grundsätzlich der Gefahr aus, daß – mit den gewünschten Programmen – versteckte Viren oder andere schädliche Programme auf den Rechner gelangen, die eine Datenmanipulation, Datenlöschung oder andere ungewollte Programmstarts bewirken.

Eine andere Gefährdung bringen Programme mit sich, die den Komfort bei der Nutzung des Browsers wesentlich erhöhen. Hier sind insbesondere ActiveX (eine Macroprogrammiersprache von Microsoft) und Java-Anwendungen (Java ist eine objektorientierte Programmiersprache von SUN Microsystems) zu nennen. Java-Anwendungen haben bei einer ordnungsgemäßen Installation zwar nur beschränkte Zugriffsrechte, bei einer falschen Rechnereinstellung ist es jedoch möglich, solche Programme von draußen zu nutzen. Über ActiveX ist unter bestimmten Voraussetzungen sogar ein uneingeschränkter Durchgriff auf die Hardware des Rechners möglich. Der Internetnutzer sollte daher in seinem Rechner die Nutzung sowohl von Java-Anwendungen als auch von ActiveX grundsätzlich sperren, solange er sie nicht benötigt. Erst dann, wenn für eine bestimmte Website – z. B. beim Homebanking – die Nutzung unerläßlich ist, kann er Java oder ActiveX hierfür entsperren und anschließend wieder sperren.

Bei den Browsern tauchen ständig neue Sicherheitsprobleme auf. Hier ist eine regelmäßige Information über die möglichen Gefährdungen und über deren Beseitigungsmöglichkeiten zwingend erforderlich. Die Beschaffung der aktuellsten Version eines Browsers kann aber auch problematisch sein, da durch neue Programmteile

ggf. neue Sicherheitsprobleme auftreten. Durch das Einspielen von sog. Patches – autorisierte Korrekturen der Hersteller – kann zumindest sichergestellt werden, daß bekannte Sicherheitslücken beseitigt werden.

Zusammenfassend ist festzustellen, daß bei der Internetnutzung ein vollständiger Schutz gegen Manipulation oder Löschung der lokalen Rechnerdaten nicht sichergestellt werden kann. Selbst die hohe Strafandrohung für Computersabotage – bis zu fünf Jahren Freiheitsstrafe nach § 303b StB G – schreckt viele Hacker nicht ab, ihr Wissen im negativen Sinne umzusetzen. Die Gefährdung kann durch rechnerseitige Sicherheitsmaßnahmen und durch diszipliniertes Verhalten des Nutzers nur reduziert werden. Zuweitgehende Sicherheitsmaßnahmen würden entsprechende Einschränkungen in der Nutzung des Internets zur Folge haben und auf wenig Gegenliebe bei den Nutzern treffen. Hier muß also ein Kompromiß gefunden werden.

Der Arbeitskreis „Technische und organisatorische Datenschutzfragen“ (AK Technik) der Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat eine „Orientierungshilfe zu Datenschutzfragen des Anschlusses von Netzen der öffentlichen Verwaltung an das Internet" erarbeitet, die die Fassung vom 1. Dezember 1995 fortschreibt und die unter meiner Homepage, http://www.bfd.bund.de, aufgerufen werden kann. Die Orientierungshilfe soll in erster Linie die für den Betrieb der Informationstechnik innerhalb der öffentlichen Verwaltung verantwortlichen Mitarbeiter unterstützen. Sie zeigt nicht nur Gefährdungen auf, sondern gibt auch Empfehlungen zu deren Abhilfe. Die Aussagen in der Orientierungshilfe lassen sich auch auf nicht-öffentliche Bereiche übertragen.

8.10 Die Kryptokontroverse

8.10.1 Nutzen und Nachteile

Es ist mehr als nur ein Wortspiel, wenn man sagt: „Kryptographie ist die Schlüsseltechnik der Datensicherheit“. Denn kryptographische Algorithmen dienen nicht nur dem Schutz von Daten gegen unbefugte Kenntnisnahme beim Transport und bei der Speicherung, sondern bilden heute auch den Kern moderner und sehr wirksamer Verfahren für

- die Versiegelung von Daten, damit jede Änderung der Daten erkannt werden kann,
- die sichere Autorisierung von Teilnehmern an digitaler Kommunikation,
- das Erzeugen einer Signatur, die so zu den signierten Daten und zum Signatar paßt, daß auch Dritte zweifelsfrei erkennen können, daß exakt diese Daten von diesem Signatar signiert wurden (vorausgesetzt, daß der Signatar die Signaturmittel nicht anderen zur Nutzung zugänglich gemacht hat),
- das Erzeugen und Handhaben von bestimmten unbekannten Trägern sicher zugeordneten Pseudonymen,
- das Prüfen von Paßwörtern ohne eine Speicherung der gültigen Paßwörter im Klartext, womit das Risiko des Auslesens der Paßwörter vermieden wird, und
- das Erzeugen und Verwalten von Daten, die wie Geld genutzt werden können, sei es in Chipkarten, sei es auf anderen Trägern.

Damit erweist sich Kryptographie als das technische Fundament nicht nur für die Gewährleistung der Vertraulichkeit von Daten und damit insbesondere für den Datenschutz, sondern auch für die Verbindlichkeit der Datenkommunikation. Mit diesem Mittel können digitale Darstellungen so gestaltet werden, daß sie wesentliche Eigenschaften klassischer Urkunden haben, was eine entscheidende Voraussetzung für die weitere Entwicklung des elektronischen Geschäftsverkehrs erfüllt.

Ähnlich nützlich erweist sich die Kryptographie aber auch zum Verbergen verbotener Aktivitäten. Denn die aus guten Gründen zur Strafverfolgung und zum Schutz der Demokratie erlaubten Eingriffe in das Post- und Fernmeldegeheimnis liefern keine brauchbaren Ergebnisse, wenn kryptographische Verfahren die Kommunikation wirksam gegen die – gesetzlich vorgesehene – Kenntnisnahme durch die zuständigen Stellen schützen. Ferner lassen sich auch Namen und Adressen von Partnern krimineller Geschäfte sowie die zugehörige Buchführung und sonstige Aufzeichnungen mit automatisierten Verfahren leicht verschlüsseln. Sie sind damit im Ernstfall weit besser vor der Aufdeckung geschützt als Notizbücher und andere klassisch geführte Unterlagen.

Unter diesen Umständen sind Bemühungen verständlich, im Interesse der allgemeinen Sicherheit den Gebrauch von Kryptographie zu verbieten, einzuschränken oder nur unter Auflagen zu gestatten, damit die befugten staatlichen Stellen von der tatsächlichen Bedeutung von gespeicherten oder kommunizierten Daten Kenntnis erlangen können, wenn dafür ein rechtfertigender Anlaß vorliegt. Eine gute Lösung, die dies ermöglicht und zugleich den Nutzen der Kryptographie für zu billigende Zwecke erhält, ist indessen jedoch nicht in Sicht.

8.10.2 Probleme einer Krypto-Regulierung

Auch wenn man die Freiheit, Nachrichten und Aufzeichnungen mit modernen Krypto-Verfahren zu verschlüsseln, nicht als unantastbares Menschenrecht ansieht, so ist es doch problematisch, von jedermann den Verzicht auf das zumindest gelegentlich durchaus sinnvolle Verbergen von Inhalten gegenüber jedem Dritten zu verlangen. Ebenso kann man nicht ohne einen sehr guten Grund verlangen, daß niemand Daten verschlüsseln darf, ohne zugleich Vorkehrungen dafür zu treffen, daß staatliche Stellen auch gegen seinen Willen und ohne sein Wissen geeignete Mittel zum Entschlüsseln anwenden können.

Das Durchsetzen von Verboten, Einschränkungen oder Auflagen wäre zudem schwierig. Denn vielen Daten, die gespeichert oder übertragen werden, kann man nicht ohne weiteres ansehen, ob die Bitfolgen kryptographisch verschlüsselte Nachrichten enthalten oder ob sie – bei verständiger Interpretation – als Klartext anzusehen sind. Das mag für Texte in gängigen Sprachen und Schriftzeichen noch einfach sein. Für Bilder, Tonfolgen und Meßwerte wäre aber, insbesondere wenn ein Komprimierungsverfahren genutzt wurde, eine intensive Be-

schäftigung mit der Bitfolge nötig, um wenigstens wahrscheinlich zu machen, daß nicht oder nicht unerlaubt verschlüsselt wurde. Eine generelle Überwachung – auch durch intensive Stichproben – würde damit zu einer bedenklichen Einschränkung des Post- und Fernmeldegeheimnisses führen. Wenn man jedoch nur Daten untersucht, die z. B. vermutlich mit einer Straftat verbunden sind, und dann feststellt, daß man wegen unerlaubter Anwendung kryptographischer Verfahren den verborgenen Inhalt nicht erkennt, müßte man sich oft lediglich mit der Verfolgung des Verstoßes gegen die Krypto-Regulierung begnügen.

Es ist aber nicht einmal sicher, daß man an einer Bitfolge zuverlässig erkennen kann, ob sie überhaupt eine geheime Nachricht verbirgt. Denn mit rechnergestützter Steganographie (verdecktes Schreiben) lassen sich Nachrichten in Daten auch für Dritte unauffindbar verstecken. Das Grundprinzip ist z. B. aus Kreuzworträtseln bekannt, in denen einige Felder mit Ziffern bezeichnet sind, die – in der angegebenen Reihenfolge gelesen – das Lösungswort oder den zu findenden Sinnspruch ergeben. Wenn man nach diesem Prinzip eine in kleine Teile zerlegte Nachricht in einer Bitfolge verstecken möchte, müssen die Positionen, an denen die Teile stehen, geheim sein. Die Positionen und ihre Reihenfolge bilden also den geheimen Schlüssel zur Nachricht.

Wählt man als Umhüllungsdaten Bitfolgen, die man unauffällig variieren kann, z. B. die Bitfolge eines ISDN-Telefongesprächs oder eines Bildes, so ist nach dem Löschen der Original-Bitfolge nicht einmal zu erkennen, daß die variierte Bitfolge kein Original ist. Denn die einzelnen kleinen Variationen entsprechen auch nur kleinen Nuancen der Tonfolge bzw. des Bildes, die genau so auch im jeweiligen Original hätten enthalten sein können. Weil Tonfolgen und Bilder heute problemlos als Daten im Internet übertragen und auf Personal-Computern gespeichert werden können, steht der entsprechend organisierten Kriminalität ein Mittel zur Verfügung, mit dem eine Krypto-Regulierung weitgehend wirkungslos gemacht werden kann.

8.10.3 Folgen der Unsicherheit

Während Krypto-Verfahren und Lösungen für das Problem der sicheren Verwaltung der geheimzuhaltenden Schlüssel entwickelt, in Programme umgesetzt und kommerziell – im Internet auch entgeltfrei – angeboten werden, ist die Frage, ob und gegebenenfalls wie eine Krypto-Regulierung geschaffen werden soll, bislang nicht verbindlich beantwortet. In den führenden Industriestaaten hat sich zwar die Ansicht durchgesetzt, daß für den Export von Krypto-Verfahren etwa die Regelungen anzuwenden sind, die für den Export von Waffen gelten, weshalb für Exporte je nach Art des Empfängerlandes bestimmte Auflagen und Beschränkungen gelten. Für die nationale Anwendung bestehen aber in den einzelnen Staaten unterschiedliche Vorschriften, wobei Deutschland zu den Staaten gehört, in denen die Nutzung der Kryptographie jedermann freisteht. Die politische Diskussion ist aber keineswegs abgeschlossen, und es besteht erhebliche Unsicherheit über die zukünftige Entwicklung.

In der Praxis führt diese Unsicherheit tendenziell zu Abwarten und zum Verzicht auf die Nutzung der verfügbaren Mittel zur Sicherung von Daten. Denn neben dem psychologischen Hindernis, in einer politisch so zweischneidigen Angelegenheit eine möglicherweise auch kritisch zu betrachtende Lösung zu wählen, bremst die Überlegung, daß eine immerhin mögliche gesetzliche Regelung die Investition in die Verfahren und die Mühen der Umstellung bald entwerten könnte.

Derartige Bedenken wirken nicht nur gegen die Nutzung von Verfahren zur Verschlüsselung von Daten, sondern z. B. auch gegen die Nutzung der digitalen Signatur. Denn die Verfahren zur Erzeugung verläßlicher digitaler Signaturen lassen sich mit geringen Variationen und unter Verwendung derselben Schlüssel auch zum Verschlüsseln von Daten nutzen. Würde nun eine Krypto-Regulierung bei entsprechendem Anlaß einer staatlichen Stelle den Zugriff auf einen der eingesetzten geheimen Schlüssel ermöglichen, so könnte diese Stelle damit auch Signaturen erzeugen, die von den „echten“ Signaturen nicht zu unterscheiden sind. Wenn man sich aber nicht absolut darauf verlassen kann, daß eine erhaltene Signatur von der als Signatar benannten Person stammt, weil auch ein Geheimdienst diese Signatur hätte erzeugen können, und wenn man sogar befürchten muß, daß die eigene digitale Signatur unbemerkt gefälscht werden kann, ist der Einsatz dieses neuen Mittels weniger erstrebenswert.

Die negativen Auswirkungen der Unsicherheit über eine eventuelle künftige Krypto-Regulierung werden allerdings die Anwendung von Kryptoverfahren für Zwecke der organisierten Kriminalität nicht stören. Denn dort sind die Kosten-Nutzen-Relationen ganz anders.

Um für die erwünschten Anwendungen der Kryptographie Entwicklungs- und Investitionssicherheit zu schaffen und damit die Anwendung dieser Techniken zum Schutz von Daten zu fördern, sollte deshalb möglichst bald Klarheit darüber geschaffen werden, ob die Nutzung solcher Verfahren gesetzlich geregelt werden soll und für welche Anwendungsbereiche gegebenenfalls Einschränkungen oder Auflagen vorgesehen sind.

8.11 „Plattencrash“ in der Garantiezeit – was tun?

Auch Festplatten sind vor Beschädigung und Zerstörung nicht sicher. Sie können auch einfach „kaputt gehen“. Zu allem Überdruß scheinen sie das immer dann zu tun, wenn auf ihnen wichtige, dringend benötigte Daten gespeichert sind, von denen es keine Sicherheitskopie gibt. Zwar kann diesem Problem durch ein geeignetes Datensicherungskonzept begegnet werden. Wenig befriedigend gelöst ist bislang aber die Frage, was mit der defekten Festplatte selbst geschehen soll – die ja noch Daten enthält! Besonders schwierig wird der Fall, wenn der „Plattencrash“ innerhalb der Garantiezeit geschieht. Ein besorgter Bürger wandte sich mit folgendem Fall an mich :

Während der Garantiezeit war auf der Festplatte seines PC ein Fehler aufgetreten, zu dessen Reparatur ihr Aus-

tausch erforderlich war. Die Lieferfirma räumte ihm zwar Garantieansprüche ein und nahm die Reparatur umgehend vor, weigerte sich aber, ihm die alte, defekte Festplatte zurückzugeben. Hiergegen protestierte der Petent jedoch, da auf der Festplatte wesentliche Teile seiner Geschäftspost und die gesamte Finanz- und Vermögensverwaltung gespeichert waren. Ihm war nämlich bekannt, daß bei Festplattendefekten in vielen Fällen zwar der „normale“ Nutzer die Daten nicht mehr lesen kann, daß es aber technisch durchaus möglich ist, die Festplatte zu reparieren und die Daten wieder lesbar zu machen. Der Petent verlangte daher alternativ die mechanische Zerstörung der Festplatte vor seinen Augen. Dies wurde mit der Begründung abgelehnt, die Platte müsse an den Hersteller zurückgeschickt werden, damit sie buchungsmäßig „gutgeschrieben“ wird. Was der Hersteller damit mache, sei nicht bekannt. Falls auf einer mechanischen Zerstörung bestanden werde, müsse er die neue Festplatte bezahlen; ein Garantieanspruch bestehe dann nicht mehr.

Auf Grund meiner Erfahrungen aus Kontrollen weiß ich, daß dies kein Einzelfall ist; immer wieder stoße ich auf ähnlich gelagerte Sachverhalte. Dies hängt zum einen damit zusammen, daß die Garantiezeit bei vielen Geräten bis zu drei Jahren beträgt und dabei mit der Ersparnis von Wartungskosten einhergeht. Die Länge der Garantiezeit wird heute als Marketingvorteil ausgenutzt. Der Kunde spart Wartungskosten und hat eventuell noch den Vorteil, daß gegen Ende einer langen Garantiezeit im Schadensfall veraltete Komponenten – die technisch längst überholt sind – durch modernere ersetzt werden.

Kritisch wird es, wenn besonders schützenswerte Daten auf der Festplatte gespeichert werden, z. B. Patientendaten. Ich empfehle daher für den Austausch von defekten Festplatten während der Garantiezeit folgendes:

1. Der sicherste und einfachste Weg, die auf Festplatten gespeicherten Daten vor unbefugter Einsichtnahme zu schützen, ist deren **kryptographische Verschlüsselung**. Hierzu gibt es am Markt verschiedene Programme, die z. T. ein sehr hohes Sicherheitsniveau erreichen und nach der Installation für den Benutzer völlig transparent ablaufen. Ich empfehle den Einsatz der Verschlüsselungsprogramme schon seit Jahren (s. u. a. 14. TB Nr. 30.3).
2. In Bereichen, in denen Verschlüsselungsprogramme aus technisch-organisatorischen Gründen – z. B. aufgrund der eingesetzten Hard- und Software – nicht eingesetzt werden können, aber die Sensibilität der Daten besondere Maßnahmen erfordert, empfehle ich den Abschluß **besonderer Vertragsbedingungen** beim Kauf eines Gerätes. So sollte darauf geachtet werden, daß diese die Vernichtung von defekten Festplatten innerhalb der Garantiezeit zusichern oder daß die defekte Platte nach dem Austausch beim Kunden verbleiben kann. Dies ist leider hin und wieder mit zusätzlichen Kosten verbunden, sollte aber aufgrund der Risiken für die gespeicherten Daten von den betroffenen Stellen in Kauf genommen werden.
3. Tritt der Defekt nach der Garantiezeit auf, wird die Festplatte in eigener Regie vernichtet.
4. In sonstigen Fällen, die es notwendig machen, die Festplatte – und damit die Daten – an eine Wartungsfirma zu geben, darf dies nur mit einer Verpflichtung der Wartungsfirma auf das Datengeheimnis (§ 5 BDSG) und gegebenenfalls Schadensersatzansprüchen erfolgen.

In diesem Sinne habe ich auch dem Petenten geantwortet und ihn gebeten, die Angelegenheit der für seine Wartungsfirma zuständigen Aufsichtsbehörde vorzutragen.

8.12 „Dienst ist Dienst und Privat ist Privat“

Schon der Volksmund sagt: „Dienst ist Dienst und Schnaps ist Schnaps“. Dies sollte in abgewandelter Form auch für die Verwendung privater PC zu dienstlichen Zwecken beherzigt werden. Der Grundsatz, dienstliche Daten nur auf dienstlichen Geräten zu verarbeiten, wird leider immer wieder durchbrochen, wie ich bei verschiedenen Kontrollen feststellen mußte. Zu welchen unerfreulichen Situationen es dabei kommen kann, habe ich schon im 16. TB unter der Überschrift „Personaldisketten im Bäckerladen gefunden“ (Nr. 18.8) berichtet.

Der Einsatz privater Geräte für dienstliche Vorgänge hängt zum einen damit zusammen, daß gerade für tragbare Geräte (Laptop, Notebook) in der Verwaltung noch ein erheblicher Nachholbedarf besteht, und viele Mitarbeiter deshalb auf private Geräte ausweichen, um z. B. während einer Dienstreise bereits die erforderlichen Dokumente zu erstellen. Zum anderen ist es manchmal auch dienstlich geboten, die begonnene Arbeit auf dem heimischen PC fortzusetzen, um beispielsweise Termine halten zu können. Die Gründe für den Einsatz privater PC zu dienstlichen Zwecken sind vielschichtig und meist im Interesse des Dienstherrn/Arbeitgebers, wie ich wiederholt feststellen konnte. Ein generelles Verbot wäre daher wenig sachgerecht.

Dies macht es erforderlich, den Einsatz privater PC für die Bearbeitung dienstlicher Vorgänge unter datenschutzrechtlichen Aspekten näher zu betrachten und zu regeln. Die Bearbeitung dienstlicher Vorgänge auf privaten PC in einer häuslichen Umgebung birgt grundsätzlich die gleichen Risiken wie die Benutzung transportabler dienstlicher PC. Die größte Gefahr, die dabei zu berücksichtigen ist, ist der Verlust der Vertraulichkeit, weil Unbefugte – Familienangehörige, Besucher usw. – von gespeicherten Daten Kenntnis nehmen können. Dieses Risiko besteht nicht nur während der Zeit, in der die Daten auf dem privaten PC verarbeitet werden und gespeichert sind, sondern auch darüber hinaus. So ist z. B. mit den standardmäßig bereitgestellten Löschbefehlen ein unwiderrufliches Löschen von Daten auf der Festplatte nicht möglich, sondern kann von Sachkundigen rückgängig gemacht werden.

Für die **dienstliche Arbeitsumgebung** wird heute in den meisten Fällen auf der Basis einer Risikoanalyse ein Sicherheitskonzept erstellt, in dem die technischen und organisatorischen Maßnahmen aufgelistet werden, die zur Herstellung einer ausreichenden Datensicherheit im Sinne des § 9 BDSG erforderlich sind. Für den **privaten Bereich** wird dieses Konzept wohl in den wenigsten

Fällen vorliegen. Trotzdem darf es nicht zu der Situation kommen, daß personenbezogene Daten – insbesondere dann, wenn es sich um besonders schützenswerte Daten, wie beispielsweise Personal- oder Gesundheitsdaten, handelt – in einem Bereich verarbeitet werden, der nur unzureichenden Schutz bietet. Ich habe deshalb in einem Rundschreiben die obersten Bundesbehörden (s. **Anlage 20**) auf die Risiken bei der Verarbeitung dienstlicher Vorgänge auf privaten PC hingewiesen und Empfehlungen für technisch-organisatorische Maßnahmen gegeben, die eine ausreichende Datensicherheit gewährleisten können.

8.13 Auf die Schutzklasse kommt es an

Das BDSG soll den einzelnen davor schützen, daß er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird (§ 1). Hierbei differenziert das Gesetz nicht zwischen Daten mit geringerem und Daten mit höherem Schutzbedarf, da sich der Schutz auf alle personenbezogenen Daten in gleichem Maße erstreckt. Weiterhin verlangt das Gesetz von jeder personenbezogene Daten verarbeitenden Stelle, die erforderlichen und angemessenen technischen und organisatorischen Maßnahmen zu treffen, um die gesetzlichen Anforderungen zu gewährleisten (§ 9 BDSG). Zur Auswahl der angemessenen Sicherheitsmaßnahmen ist es in allen Fällen zunächst notwendig, sich einen genauen Überblick über die Sicherheitsanforderungen zu verschaffen, die auf Grund der zu schützenden Daten und der eingesetzten IT-Systeme notwendig sind. Neben diesen primären Faktoren müssen bei der Entscheidung über die angemessenen Maßnahmen noch weitere Gesichtspunkte beachtet werden. Eine wesentliche Rolle spielt dabei der Kontext, in dem die Daten stehen. So wäre z. B. eine Parkplatzdatei meiner Dienststelle sicherlich weniger schützenswert, als die Parkplatzdatei des Bundesnachrichtendienstes, obwohl in beiden Dateien die gleiche Art von Daten gespeichert wäre. Ebenso müssen u. a. die Infrastruktur, die Anzahl der gespeicherten Datensätze, die Speicherdauer oder das Speichermedium berücksichtigt werden, um die angemessenen Schutzmaßnahmen bestimmen zu können. Nimmt man alle denkbaren Faktoren, entsteht ein sehr komplexes Beziehungsgeflecht, das eine Bewertung der Sicherheitsanforderungen äußerst aufwendig gestaltet. Ein pauschaliertes Zuordnen der Daten – etwa zu „*gering, mittel-, hochsensibel*" – erscheint problematisch, weil die Gefahr besteht, daß hierdurch wesentliche datenschutzrechtliche Schutzaspekte – beispielsweise der Kontext, in dem diese Daten stehen – verloren gehen. Gleichwohl ist ein Bedarf für sachgerechte Vorgaben hinsichtlich der Einordnung von Daten in „Schutzklassen" nicht zu verkennen, denn solche Verfahren sind einfach in der Anwendung und – bei richtiger Gestaltung – sicherheitsfördernd.

Ich unterstütze daher ein entsprechendes Konzept der Bundesregierung. Die „Empfehlung der Koordinierungs- und Beratungsstelle der Bundesregierung für Informationstechnik in der Bundesverwaltung (KBSt) zur Anwendung eines Schutzklassenkonzepts" (GMBl 1998 Nr. 1 Seite 3ff.) sieht ein mehrstufiges Schutzklassenkonzept vor und teilt hierfür die Daten nach ihrem Schutzbedarf ein. Das Konzept sieht drei Schutzklassen vor – gering bis mittel, hoch, sehr hoch –, deren Definition auch mit Beispielen von personenbezogenen Daten ergänzt wird. Die zu den Schutzklassen genannten Beispiele sollen dabei nicht als strenge Vorgaben, sondern nur als Richtschnur gesehen werden. Die Einteilung in Schutzklassen soll letztlich nur den Weg zur richtigen Maßnahmenauswahl erleichtern. Aus meiner Sicht entscheidend ist, daß die KBSt in der aufgezeigten Vorgehensweise (s. Abbildung 7) meiner grundsätzlichen Haltung

– Verarbeitung personenbezogener Daten erfordert „Grundschutz + X" –

(s. 14. TB Nr. 30.8) – Rechnung trägt. Im Einzelfall sind weiterhin die näheren Umstände der Verarbeitung in die Betrachtung miteinzubeziehen. Ich hoffe, daß das Schutzklassenkonzept die Verantwortlichen der datenverarbeitenden Stellen wirksam bei der Realisierung der erforderlichen Sicherheitsmaßnahmen unterstützen und somit zu einem besseren Sicherheitsniveau beitragen kann.

8.14 Der Bürger als Versuchskaninchen

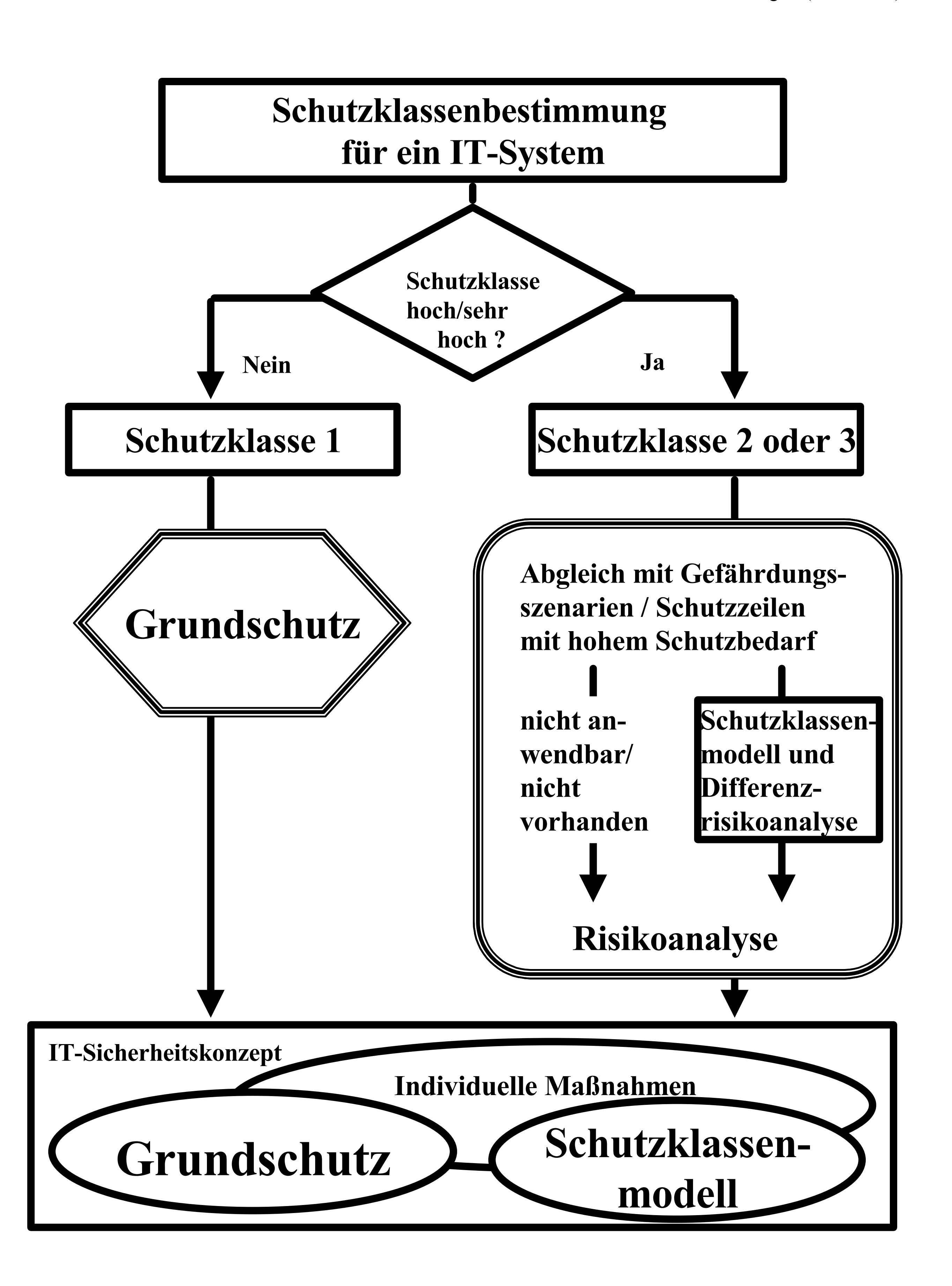
Bei der Entwicklung von Software und von Schnittstellen zwischen Datenverarbeitungssystemen, aber auch zur Beseitigung von Programmfehlern ist es notwendig, die Leistungsfähigkeit dieser Systeme mit Funktionstests unter möglichst realitätsnahen Bedingungen zu überprüfen. Diese Tests werden häufig bereits während der Entwicklung, spätestens aber vor der Übergabe der Systeme an die Anwender durchgeführt. Um spätere Systemfehler zu vermeiden, erfolgt dies zweckmäßigerweise mit einem dem originalen Datenbestand vergleichbaren **Testdatenbestand**. Dieser enthält keine echten Daten z. B. von wirklichen Kunden einer Firma, sondern sogenannte „dummy"-Daten, also solche Daten nicht existierender künstlicher Personen – beliebt sind hier auch literarische und Comic-Figuren.

Leider muß ich in der Praxis jedoch häufig feststellen, daß nicht Testdaten, sondern – der Einfachheit halber – Kopien des **Originaldatenbestandes** für diese Tests herangezogen werden. In einem Fall waren dabei Veränderungen in den Datensätzen vorgenommen und dann durch einen Fehler wieder im Originaldatensatz gespeichert worden. Der Fehler wurde erst durch einen falschen Zahlungsbescheid entdeckt und konnte nur mit einem erheblichen Aufwand behoben werden. In einem anderen Fall wurde sogar mit den Originaldaten selbst getestet.

Diese Praxis ist äußerst problematisch, weil das IT-Personal der Behörde und/oder des mit der Softwareentwicklung beauftragten externen Unternehmens dadurch an vertrauliche Informationen über Bürger gelangen.

Auch wegen der im Testbetrieb noch vorhandenen Unsicherheiten dürfen in der Entwicklungsphase und der anschließenden Testphase – d. h. vor Freigabe eines Programms bzw. eines Systems durch die fachlich zuständige Organisationseinheit – nur Daten verarbeitet

Abbildung 7 (zu Nr. 8.13)



werden, die keinen Personenbezug im Sinne von § 3 Abs. 1 BDSG haben. Die Verarbeitung von Echtdaten in der Testphase ist nach § 9 i.V.m. der Anlage zu § 9 Satz 1 und § 18 BDSG unzulässig und wird von mir in der Regel nach § 25 Abs. 1 BDSG beanstandet.

8.15 Ausschluß unzuverlässiger Unternehmer von der Vergabe öffentlicher Aufträge

In der 13. Legislaturperiode beschloß die Bundesregierung, Maßnahmen zur Bekämpfung der Korruption einzuleiten. Denn eine Vertragspartnerschaft der öffentlichen Hand mit einem Unternehmen, das durch Korruption oder Preisabsprachen Einfluß auf die Vergabeentscheidung zu nehmen versucht, ist für den Staat unzumutbar. Deshalb sollte ein Kabinettsbeschluß über den Ausschluß von unzuverlässigen Unternehmern bei der Vergabe von öffentlichen Aufträgen verabschiedet werden.

Es war geplant, in dem Kabinettsbeschluß u. a. die Einrichtung eines zentralen Registers über Unternehmen zu regeln, die in Korruption und Preisabsprachen verwickelt waren. Das Register sollte neben belastenden Daten den Namen und die Adresse des Unternehmens, aber auch von natürlichen Personen, z. B. von unzuverlässigen leitenden Mitarbeitern des Unternehmens, enthalten. Alle mit der Vergabe von öffentlichen Aufträgen betrauten Stellen sollten Zugriff auf das zentrale Register erhalten. Dazu ist es jedoch in der 13. Legislaturperiode nicht mehr gekommen.

Da eine Vergabe von Aufträgen im Allgemeininteresse liegt und eine Beschränkung der Datenschutzrechte der Betroffenen aus Gründen des Allgemeininteresses gerechtfertigt werden könnten, hätte die erforderliche Verarbeitung von personenbezogenen Daten auch gesetzlich geregelt werden können. Statt für diese Verarbeitung von personenbezogenen Daten eine gesetzliche Grundlage zu schaffen, war beabsichtigt, von allen Unternehmen mit den Ausschreibungsunterlagen eine entsprechende Einwilligungserklärung zu verlangen.

Eine solche Lösung hätte zwei Nachteile:

Zum einen ist es ein zweifelhafter Umgang mit dem Recht auf Selbstbestimmung, wenn man den Betroffenen zu einer Einwilligung zwingt, zum anderen könnte der Betroffene seine gegebene Einwilligung jederzeit gegenüber den zuständigen Stellen widerrufen, mit dem Ergebnis, daß jede weitere Verarbeitung seiner Daten – mit Ausnahme der Löschung – unzulässig wäre. Darüber hinaus sah die Regelung vor, daß die betroffenen Unternehmen eine Selbstauskunft aus dem Gewerbezentralregister vorlegen sollten, wenn sie an einer öffentlichen Ausschreibung teilnehmen. Die Verpflichtung zu einer solchen Selbstauskunft ist aber weder in der Gewerbeordnung noch in einer anderen einschlägigen Regelung enthalten. Aufgrund dieses Einwandes meinerseits wurde der entsprechende Abschnitt in dem Entwurf des Beschlusses gestrichen. Eine wirksame und zugleich datenschutzgerechte Regelung zum Ausschluß unzuverlässiger Unternehmen von der Vergabe öffentlicher Aufträge steht damit noch aus.

Anfang des Jahres 1999 hat mich das BMWi darüber informiert, durch eine gesetzliche Regelung, die als Ermächtigung zum Erlaß einer Rechtsverordnung in § 127 GWB eingefügt werden könnte, eine tragfähige Rechtsgrundlage für Maßnahmen zum Ausschluß unzuverlässiger Unternehmer von der Vergabe öffentlicher Aufträge zu schaffen. Der Entwurf bleibt abzuwarten.

9 Chipkarten

Die Möglichkeiten, auf einem Chip nicht nur Daten, sondern auch einen Prozessor unterzubringen, der diese Daten verwaltet und durch im selben Chip gespeicherte Sicherungsprogramme die Ein- und Ausgabe der Daten kontrolliert, machen Chipkarten zu einem interessanten Mittel für unterschiedliche Anwendungen. Denn mit der weiter fortschreitenden Miniaturisierung werden sowohl die Speicherkapazitäten als auch die Leistungsfähigkeit der Prozessoren erheblich vergrößert, ohne daß sich die Gesamtkosten einer Chipkarte besonders erhöhen. So dürften Chipkarten mit einer Million Bytes Speicherkapazität bald ein Massenprodukt sein, und der z. B. bei den Telefonkarten gelegentlich auftretende Effekt, daß Verschmutzungen oder Beschädigungen der Kontakte die Nutzung verhindern, wird in wenigen Jahren durch kontaktlose Datenübertragung zwischen Karte und Terminal vermieden werden.

Neben den Konsequenzen, die sich aus der allgemeinen Entwicklung der Chipkarten und ihrer Nutzung für die Novellierung des BDSG ergeben (s. o. Nr. 2.1.2), sind vor allem die Folgen des Chipkarteneinsatzes im Gesundheitswesen und im Zahlungsverkehr zu beachten.

9.1 Chipkarten für Gesundheitsdaten

Bei der Behandlung eines Patienten kann dessen Chipkarte hilfreich sein, wenn sie für den Arzt wesentliche Angaben zur Gesundheit des Patienten enthält. Über die Vorteile dieser Unterstützung und die Arbeiten, die zur Realisierung entsprechender Projekte durchgeführt werden, sowie über die Vorkehrungen zum Schutz dieser Daten gegen unbefugte Nutzungen habe ich in meinem 16. TB (Nr. 9.2) ausführlich berichtet. Die dort beschriebenen Arbeiten insbesondere an der Definition eines Kerndatensatzes und anderen Festlegungen, die für das Zusammenwirken von Karten der Patienten mit den DV-Systemen der Ärzte und anderen Leistungserbringern erforderlich sind, wurden national und international fortgesetzt. Ferner wurden in verschiedenen Studien-, Modell- und Pilotprojekten die Durchführbarkeit und die Akzeptanz positiv getestet. Dabei ist besonders der Einsatz von Patientenkarten in der Nierenersatztherapie sowohl zur individuellen Patientenbetreuung als auch zur praxisübergreifenden Qualitätssicherung hervorzuheben. Hier sind schon über 30 000 Karten an die Patienten ausgegeben, die aber erst ab Mai 1999 im geplanten Umfang genutzt werden.

9.1.1 Verzögerungen bei der Anwendung

Trotz der durchaus erfolgreichen Arbeiten an der Planung ist zur Zeit kein konkretes nationales Projekt bekannt, mit dem ein Systemanbieter eine Karte über-

regional und unabhängig von speziellen Therapien allgemein anbieten möchte. Angesichts der großen Möglichkeiten, die Chipkarten für Patientendaten bieten, bleibt damit die Entwicklung insgesamt etwas hinter den hochgespannten Erwartungen zurück. Das liegt im wesentlichen daran, daß die einzelnen Schritte sich als mühsamer und langwieriger in der Detailplanung und in der Realisierung erweisen, als es zunächst erwartet wurde. So ist z. B. die **Health Professional Card** (HPC), deren Nutzung eine wesentliche Voraussetzung für den sicheren Umgang mit allgemeinen Patientendatenkarten ist (s. 16. TB Nr. 9.1.2) noch nicht eingeführt, u. a. weil es nach dem Inkrafttreten des **Signaturgesetzes** am 1. August 1997 noch über ein Jahr dauerte, bis entsprechende Produkte einsetzbar waren, und weil ein abgestimmtes Konzept dafür fehlt, wie nicht nur Ärzte, sondern auch Angehörige anderer Gesundheitsberufe ihre HPC erhalten. Außerdem fehlt noch immer ein Gesetzentwurf für den gebotenen rechtlichen Schutz der Gesundheitsdaten auf Patientenkarten, den der Deutsche Bundestag in seinen Beschlüssen zu meinem 15. und zu meinem 16. TB gefordert hat (s. **Anlage 4**). Dieser Gesetzentwurf dürfte die Investitionssicherheit deutlich erhöhen.

9.1.2 Gesundheitsdaten auf die Krankenversicherungskarte?

Inzwischen überlegen die Krankenkassen und ihre Verbände, welche Eigenschaften die nächste Generation der vor vier Jahren eingeführten **Krankenversichertenkarte** (KVK) haben sollte, die zur Zeit nur die früher verwendeten Krankenscheine ersetzt.

Neben Sicherungsfunktionen, die das unbefugte Ändern der Daten im Chip verhindern sollen (s. dazu schon 14. TB Nr. 12.4), wird z. B. erwogen, alle Arztbesuche des laufenden Quartals zu registrieren, um damit zu verhindern, daß unangemessen und unwirtschaftlich viele Arztbesuche in kurzer Zeit stattfinden. Die Vermutung, daß dadurch relevante Einsparungen möglich würden, ist jedoch nicht belegt, aussagefähige Untersuchungen dazu liegen nicht vor. Es gibt auch keine versicherungsrechtliche Begrenzung des Rechts auf freie Wahl des Arztes, die eine mutwillige Überdehnung dieses Rechts zu Lasten der Krankenkasse verhindert. Erst wenn eine solche Begrenzung existiert, sollte erwogen werden, ob die KVK das geeignete Mittel ist, um einen Nachweis über diese Sachverhalte zu führen. Denn die Kassen, die nach der Ausgabe der KVK darauf keinen Zugriff haben, bekommen die Daten ohnehin im Rahmen der Quartalsabrechnungen. Zudem müßten solche Daten auf der KVK – anders als die Versicherungsangaben – besonders gegen unbefugte Kenntnisnahme gesichert werden, weil sie Hinweise auf die Gesundheit des Versicherten geben.

Eine naheliegende und seit einigen Jahren diskutierte Erweiterung der KVK-Funktionen ist ihre Nutzung als Träger für ein **elektronisches Rezept**:

Wenn der Patient die Daten des Rezepts auf seiner KVK zur Apotheke bringt, wo sie automatisiert gelesen und verarbeitet werden können, läßt sich Verwaltungsarbeit einsparen. Eine der technischen Voraussetzungen dafür ist, daß die Daten, die das Rezept darstellen, durch eine digitale Signatur des verschreibenden Arztes gegen Fälschung und Verfälschung gesichert sind; eine andere ist, daß die Daten nur von dazu befugten Personen bzw. deren Lesegeräten ausgelesen werden können. Für beides wären HPC für Ärzte und Apotheker geeignete Mittel. Weil außerdem ein konkretes, unter den Beteiligten abgestimmtes Konzept für ein elektronisches Rezept noch nicht vorliegt, ist kaum damit zu rechnen, daß schon bei dem in nächster Zeit anstehenden Austausch der ersten KVK, deren Gültigkeitsdauern demnächst enden, KVK ausgegeben werden können, die auch dafür geeignet sind.

Noch weiter in die Zukunft reichen Überlegungen, auf der KVK neben eher verwaltungsnahen Funktionen noch allgemeine Angaben zur Gesundheit des Versicherten zu speichern. Das Hauptargument dafür ist, daß der Versicherte dann nur eine Karte für die Versicherungs- und für seine Gesundheitsdaten braucht. Das Hauptargument dagegen ist, daß er dann nur noch eine Karte hat, die er auch dort und dann vorlegen müßte, wo und wenn er seine Gesundheitsdaten gerade nicht präsentieren möchte. Um seine Freiheit zu gewährleisten, über das Bekanntgeben seiner Gesundheitsdaten selbst und ohne Druck zu entscheiden, ist eine **Gesundheitsdatenkarte**, deren Besitz freiwillig ist und die man auch dann nicht vorlegen muß, wenn man sie hat, eine solide Lösung. Für zukünftige **multifunktionale Chipkarten** ist zwar vorstellbar, daß völlig getrennt von der Funktion KVK die Funktion Gesundheitsdatenkarte auf einem gemeinsamen Träger realisiert wird. Dabei müßte technisch gewährleistet sein, daß gegen den Willen des Patienten niemand auch nur feststellen kann, ob überhaupt irgend welche Gesundheitsdaten in der Karte gespeichert sind, die er als KVK präsentiert. Bevor diese Trennung überzeugend gewährleistet ist, sollte man diese Vereinfachung nicht propagieren.

Alle diese Erweiterungen der in der KVK zu speichernden Daten der Versicherten werden nur zulässig, wenn u. a. der in **§ 291 SGB V** gesetzlich festgelegte **Datenkatalog** geändert wird. Auch deshalb müßten zunächst aus den Ideen überzeugende Konzepte für nützliche Verbesserungen erarbeitet werden.

9.2 Die Geldkarte

Wenn es nach den Banken ginge, dann gibt es wohl in einigen wenigen Jahren fast kein Bargeld mehr – diesen Eindruck läßt jedenfalls deren Werbung entstehen. Das Bezahlen der lästigen Kleinbeträge am Kiosk, im Taxi oder im Parkhaus, im öffentlichen Personennahverkehr oder im Schwimmbad, das bislang aus Handhabungs- und Kostengründen mit einer Kreditkarte nur schwer möglich war und zudem teuer ist, soll dann möglichst mit einer simplen Plastikkarte, der „Geldkarte“ erfolgen. Das erklärte Ziel der Geldkarte ist der Ersatz des Kleingeldes, der Münzen. Das Bezahlen soll einfacher, schneller und bequemer werden. Kein lästiges Hantieren mit Münzgeld, kein Warten in einer Schlange im Zeitschriftenladen oder beim Busfahrer mehr, weil man nicht

das passende Kleingeld hat. Die neuen EC- und Kreditkarten fast aller Kreditinstitute haben schon den Chip, mit dem sie zur Geldkarte werden.

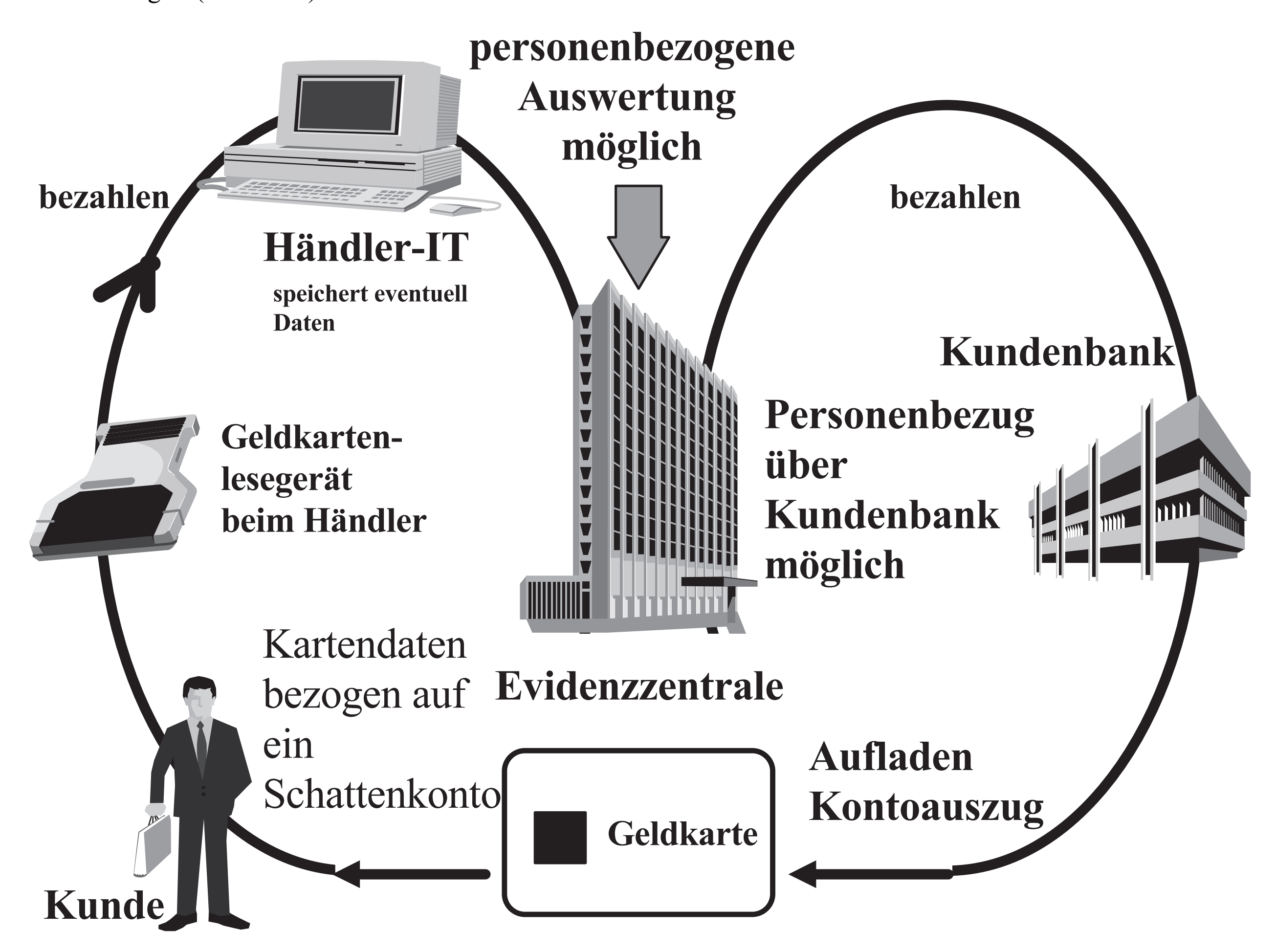
Auch ein Datenschutzbeauftragter freut sich, wenn der Alltag etwas bequemer wird. Die Geldkarte muß ihm aber auch Sorgen machen. Denn eine gute Eigenschaft des typischen Kleingeld-Bezahlvorgangs, nämlich seine **Anonymität**, geht mit der Geldkarte verloren (s. auch **Anlage 13**).

9.2.1 Auf dem Weg zum „Gläsernen Kunden“?

Das technische Konzept, das der Zentrale Kreditausschuß (ZKA) erarbeitet hat, sieht für die Nutzung der Karte eine jahrelange Speicherung aller Daten über Veränderungen des in einer Geldkarte nachgewiesenen Betrages (Bewegungsdaten) vor. So speichert schon die Karte neben den Kartenbasisdaten (Kartennummer, Guthaben, Bankleitzahl der Kundenbank, Kartenverfallsdaten) bis zu 15 Datensätze über Zahlungsvorgänge mit folgendem Inhalt: Betrag der Buchung, neuer Guthabenbetrag auf der Karte, Datum und Uhrzeit der Buchung, die Händlerkennung und die Art des Vorgangs (Buchen, Rückbuchen).

Im Händlerterminal wird ein Datensatz erzeugt und gespeichert, der außer diesen Informationen noch Sicherungsdaten zum Beweis der Richtigkeit der Angaben enthält. Er wandert anschließend – über die Bank des Händlers oder andere Clearingstationen – in die sogenannte Evidenzzentrale. Dorthin gelangen auch entsprechende Daten über das Auffüllen des Geldvorrates auf der Geldkarte, was am Bankschalter oder an besonderen Geldautomaten möglich ist und „Laden“ genannt wird. Die Evidenzzentrale prüft, ob die eingereichten Datensätze korrekt sind und nicht schon früher einmal vorgelegt wurden, und sie sorgt – bei positivem Ergebnis – dafür, daß der Händler zu seinem Geld kommt. Außerdem speichert sie alle Bewegungsdatensätze für mindestens sechs Jahre. Die Evidenzzentrale kann damit bei Bedarf im Zusammenwirken mit der Kundenbank Kauf- und Bewegungsprofile des Geldkartenbenutzers erzeugen (s. Abb. 8).

Abbildung 8 (zu Nr. 9.2)



Wenn dieses Zahlungssystem sich am Markt durchsetzen und auch für Zahlungen im elektronischen Handel genutzt werden sollte, dann würden in wenigen Jahren hunderte Millionen von Datensätzen das Konsumverhalten der Bürger beschreiben. Von der Zahlung am Automaten (z. B. für Getränke, Fahrkarten, Süßigkeiten oder Zigaretten), am Frittenstand, in der Kantine, im Internet oder im Parkhaus bis hin zum Zeitungskauf am Kiosk könnten Einzeldaten über das Konsumverhalten der Bürger, in vielen Fällen bis hin zum persönlichen Tagesrhythmus, noch Jahre später ausgewertet werden:

Ein großer, schlechter Schritt hin zum gläsernen Kunden.

9.2.2 Kürzere Löschungsfristen für Kundendaten

Auch Vertreter der Banken haben gewisse Zweifel, ob es wirklich sinnvoll ist, Daten über die einzelnen Zahlungen mit der Geldkarte in dem oben beschriebenen Ausmaß zu sammeln. Wenn man sich schon nicht für ein Verfahren entscheidet, bei dem solche Daten gar nicht erst anfallen (s. 16. TB Nr. 9.3.2), so wäre als Alternative z. B. eine Löschung der Daten über die einzelnen Kundenzahlungen dann denkbar, wenn sie – nach allen Prüfungen und nach der Abrechnung mit den Händlern – nicht mehr benötigt werden. An einer so frühen Löschung sieht man sich jedoch durch handels- und steuerrechtliche Vorschriften gehindert.

Deshalb habe ich mich an das BMF gewandt, die Vorteile einer schnellen Löschung der Einzelzahlungsdaten beschrieben und gebeten, mir mitzuteilen, was aus seiner Sicht dieser Verbesserung des Verfahrens entgegensteht. Weil das derzeitige System der deutschen Geldkarte offensichtlich nicht dem Leitbild für die Informationsgesellschaft entspricht, das der Deutsche Bundestag in Nr. 2 seiner Entschließung zu meinem 16. Tätigkeitsbericht herausgestellt hat (s. **Anlage 4**), hatte ich gehofft, daß auch das BMF eine Verkürzung der Speicherungsfristen für sinnvoll halten könnte.

Die Antwort des BMF war jedoch eher enttäuschend:

Zu der vom Deutschen Bundestag für vorbildlich gehaltenen datenschutzfreundlichen Tendenz des Informations- und Kommunikationsdienste-Gesetzes enthielt sie die Meinung, dieser *„bedenklichen Entwicklung“* müsse *„Einhalt geboten werden“*. Die Folge, daß wegen der greifenden handels- und steuerrechtlichen Aufbewahrungspflichten das Kontrollpotential besonders groß ist, wurde als positiv bewertet. Deshalb sei dieses System im Vergleich zu solchen, die mit weniger personenbezogenen Daten auskommen, sowie im Vergleich zu Bargeld vorzuziehen.

Nun richtet sich das steuerliche Interesse gerade bei Kleingeldzahlungen aber nicht auf den zahlenden Kunden, sondern auf denjenigen, der dabei – steuerlich relevante – Einnahmen erzielt. Die Einnahme-Daten liefert das Clearing-System der deutschen Geldkarte jedoch völlig unabhängig davon, wie lange die Kundendaten nach der Prüfung und Abrechnung noch gespeichert sind. Das Anlegen riesiger Datensammlungen über Kunden ist mit der steuerlichen Relevanz der Einnahmen also nicht zu begründen. Deshalb habe ich meine Vorstellungen dem BMF noch einmal ausführlich dargelegt. Bis Redaktionsschluß stand seine Antwort noch aus.

10 Telekommunikation

10.1 Telekommunikationsrecht

10.1.1 TKG-Begleitgesetz: (K)ein Meilenstein im Datenschutz?

Im Jahr 1996 wurden mit dem Telekommunikationsgesetz die erforderlichen gesetzgeberischen Maßnahmen zur Herstellung von Wettbewerb im Telekommunikationsmarkt geschaffen (s. 16. TB Nr. 10.1). Aus Zeitgründen konnte bei der Verabschiedung des Gesetzes das sonstige Bundesrecht nicht angepaßt werden, obwohl es notwendig gewesen wäre. Erst ein Jahr später, 1997, im Rahmen des Begleitgesetzes zum Telekommunikationsgesetz (TKG-Begleitgesetz) vom 17. Dezember 1997 wurden die erforderlichen Änderungen und Ergänzungen verabschiedet.

Mit Artikel 1 TKG-Begleitgesetz wurden die erforderlichen personalrechtlichen Voraussetzungen für die Errichtung der Regulierungsbehörde für Telekommunikation und Post geschaffen. Artikel 2 regelt die in verschiedenen Bereichen erforderlichen gesetzlichen Änderungen im Hinblick auf die mit der Postreform vollzogene Privatisierung und Liberalisierung im Bereich der Telekommunikation; diese Vorschriften sind für den Datenschutz im Bereich der Telekommunikation von wesentlicher Bedeutung. Die wichtigsten Anliegen des Gesetzgebers bei der Anpassung von Rechtsvorschriften galten

- einer weitgehenden Angleichung rechtlicher Rahmenbedingungen für die Nachfolgeunternehmen der Deutschen Bundespost und deren Wettbewerber,
- dem Schließen von Strafbarkeitslücken bei der Verletzung des Fernmeldegeheimnisses sowie
- der Sicherstellung der Überwachbarkeit von Telekommunikation durch die dazu berechtigten Behörden.

Im Verlauf des Gesetzgebungsverfahrens sind insbesondere die Regelungen zur **Überwachung der Telekommunikation** intensiv diskutiert worden.

So habe ich große Bedenken gegen die in Artikel 2 Abs. 1 Nr. 1b TKG-Begleitgesetz vorgenommene Ausdehnung der staatlichen Eingriffsbefugnisse nach dem G 10-Gesetz auf sog. **geschlossene Benutzergruppen**. Im Gegensatz zu den Betreibern von öffentlichen, für jedermann zugänglichen Telekommunikationsdiensten versteht man darunter solche, die TK-Dienste ausschließlich für bestimmte Personen oder Organisationen anbieten. Typisch für solche „Corporate Networks“ sind etwa die konzerneigenen TK-Netze großer, auch weltweit operierender Wirtschaftsunternehmen. Diesen hinzuzurechnen sind nach dem Willen des Gesetzgebers aber auch Nebenstellenanlagen wie beispielsweise in Hotels und Krankenhäusern, Clubtelefone sowie Neben-

stellenanlagen in Betrieben und Behörden, soweit diese den Beschäftigten zur privaten Nutzung zur Verfügung gestellt werden.

Eine inhaltsgleiche Vorschrift war bereits für die Änderung des G 10-Gesetzes vom 28. April 1997 angedacht worden. Schon im damaligen Gesetzgebungsverfahren habe ich Bedenken gegen diese Bestimmung geltend gemacht und konnte erreichen, daß einvernehmlich auf die beabsichtigte Ausdehnung der Eingriffsbefugnisse auf geschlossene Benutzergruppen verzichtet wurde. Statt dessen ist in Artikel 1 § 1 Abs. 2 des G 10-Gesetzes die Formulierung *„Unternehmen, die Telekommunikationsdienstleistungen für die Öffentlichkeit erbringen"* gewählt worden. Es wäre im Interesse eines effektiven Datenschutzes besser gewesen, diesen Rechtszustand im TKG-Begleitgesetz nicht aufzugeben. Dies gilt insbesondere für den sensiblen Bereich der Nebenstellenanlagen in Krankenhäusern, die in der Regel nicht nur dem Klinikpersonal, sondern auch ihren Patienten die Möglichkeit bieten, die TK-Anlage zu nutzen.

Leider wurden auch durch die entsprechenden Änderungen der **Strafprozeßordnung** und des **Außenwirtschaftsgesetzes** (Artikel 2 Abs. 9 bzw. 23 TKG-Begleitgesetz) die Befugnisse staatlicher Stellen, die Telekommunikation überwachen zu dürfen, auf die geschlossenen Benutzergruppen ausgedehnt.

Auch der von der Bundesregierung beabsichtigten Ergänzung der Strafprozeßordnung konnte ich nicht zustimmen. Die vorgesehene Vorschrift eines neuen § 99a StPO sollte den bisherigen **§ 12 FAG** ersetzen, der die Auskunftspflicht von TK-Unternehmen gegenüber der Justiz regelt. So enthielt der Entwurf des § 99a StPO keine Schutzklausel für Telefonate von Personen, die zur **Wahrung des Berufsgeheimnisses** verpflichtet sind, wie z. B. von Ärzten und Rechtsanwälten. Auch fehlte eine Regelung über die Vernichtung der für die Strafverfolgung nicht erforderlichen Daten und über die Unterrichtung der von der Maßnahme nach § 99a StPO betroffenen Personen. (Weitere Einzelheiten s. o. Nr. 6.4 Zugriff der Strafverfolgungsbehörden auf Telekommunikationsdaten – Neufassung des § 12 FAG?).

Meine im Gesetzgebungsverfahren vorgetragenen Bedenken konnten letztlich von der Bundesregierung nicht ausgeräumt werden. Der Bundestag hat daher von der Ergänzung der StPO um § 99a Abstand genommen. Gleichzeitig hat er der Bundesregierung aufgegeben, unter besonderer Berücksichtigung der datenschutzrechtlichen Aspekte bis zum 31. April 1998 einen neuen Entwurf eines § 99a StPO zu erarbeiten. Trotz entsprechender Anfragen liegt mir bis heute noch keine neue Fassung für § 99a StPO vor. Wegen der notwendigen gründlichen Beratungen mit den Ressorts und in den parlamentarischen Gremien ist dies jedoch schwer verständlich. § 12 FAG als Vorgängervorschrift des § 99a StPO ist bis zum 31. Dezember 1999 befristet.

Besondere Irritationen in der Öffentlichkeit hat die im Rahmen des Gesetzgebungsverfahrens geführte Diskussion zum sog. **IMSI-Catcher** ausgelöst. Obwohl der Einsatz des IMSI-Catchers letztlich nicht Gegenstand des Gesetzgebungsverfahrens geworden ist, möchte ich wegen der öffentlichen Diskussion und im Hinblick auf mögliche künftige Begehrlichkeiten hierzu folgendes anmerken:

Beim IMSI-Catcher handelt es sich um ein Gerät, mit dem die Telefonnummern in der Nähe befindlicher Mobiltelefone identifiziert werden können, die zu diesem Zeitpunkt empfangsbereit geschaltet sind, mit denen jedoch nicht telefoniert wird. IMSI bedeutet International Mobile Subscriber Identity. Es wird also eine Nummer „gefangen", die es ermöglicht, auch die unbekannte Telefonnummer des Handy zu ermitteln, die ein Verdächtiger benutzt.

Dies wurde in der Öffentlichkeit vielfach dahingehend mißverstanden, daß nicht nur die Rufnummern ermittelt, sondern auch die geführten Gespräche abgehört werden sollen. Auch wenn lediglich die Telefonnummern der Mobiltelefone – z. B. von der Polizei – ermittelt werden sollten, so wäre dies doch ein ganz erheblicher Eingriff in das Fernmeldegeheimnis der Betroffenen. Der IMSI-Catcher ermittelt aber – technisch unvermeidbar – neben der Rufnummer verdächtiger Personen auch die Rufnummern völlig Unbeteiligter. Um aber feststellen zu können, wer tatsächlich unbeteiligt ist, wären eben auch Ermittlungen im Umfeld all derer erforderlich, deren IMSI „mitgefangen" wurde. Das hätte aus meiner Sicht zu unverhältnismäßigen Eingriffen in das Persönlichkeitsrecht geführt.

Das vom Bundesrat sogar angedachte **Mithören von Gesprächsinhalten** mittels des IMSI-Catchers wäre ein eklatanter Verstoß gegen das Recht auf unbeobachtete Kommunikation gewesen. Dank der heftigen öffentlichen Diskussion, aber auch der Mahnungen aus dem Bereich der TK-Unternehmen und der seinerzeit noch bestehenden Fernmeldeverwaltung wurden die Pläne der Bundesländer nicht weiterverfolgt.

Dem Bundesgesetzgeber ist mit dem TKG-Begleitgesetz zwar die dringend gebotene Harmonisierung von Rechtsvorschriften gelungen. Für den Bürger und für den Kunden von Telekommunikationsdienstleistungen ist damit ein Stück Rechtssicherheit geschaffen worden. Gleichwohl bedeuten die Bestimmungen zur Überwachung der Telekommunikation einen datenschutzrechtlichen Rückschritt. Ich werde mich bei der Umsetzung der EG-Telekommunikations-Datenschutzrichtlinie in deutsches Recht (vgl. Nr. 10.1.4) für entsprechende Korrekturen einsetzen.

10.1.2 Telekommunikations- und Teledienste – Verwirrung vorprogrammiert!

Am 1. August 1997 sind im Rahmen des IuKDG das Teledienstegesetz (TDG) sowie das Teledienstedatenschutzgesetz (TDDSG) in Kraft getreten. Nach § 2 Abs. 1 TDG handelt es sich bei Telediensten um elektronische Informations- und Kommunikationsdienste, die für eine individuelle Nutzung von kombinierbaren Daten, Bildern oder Tönen bestimmt sind und denen eine Übermittlung mittels Telekommunikation zugrunde liegt. Da diese Begriffsbestimmung sehr abstrakt gehalten ist, hat der Gesetzgeber in § 2 Abs. 2 TDG einige

Teledienste beispielhaft aufgezählt. Genannt sind dabei unter anderem das Telebanking, die Nutzung des Internets sowie das Teleshopping.

Mit dieser technisch orientierten Definition wollte der Gesetzgeber deutlich machen, daß bei dem Erbringen eines Teledienstes stets auch „ein Stück“ Telekommunikationsdienst geleistet wird. Die Telekommunikation kann quasi als „Transportebene“ verstanden werden, auf der der Teledienst erfolgt. Für die bei der Nutzung eines Teledienstes zu verarbeitenden Verbindungsdaten stellt sich daher die Frage, wann das TDDSG als das den Teledienst betreffende bereichsspezifische Datenschutzgesetz und wann das für die den Teledienst tragende Telekommunikation einschlägige Telekommunikationsgesetz (TKG) eingreift. Neben Unterschieden im materiellen Recht hat dies auch Auswirkung auf die datenschutzrechtliche **Kontrollkompetenz**. Gemäß § 91 Abs. 4 TKG obliegt mir die Aufsicht für den Bereich der Telekommunikation. Demgegenüber sind für die Datenschutzkontrolle der Teledienste gemäß § 8 TDDSG die Aufsichtsbehörden im nicht-öffentlichen Bereich nach § 38 BDSG zuständig.

Der Gesetzgeber hat weder dem Telekommunikationsdatenschutz noch dem Teledienstedatenschutz einen generellen Vorrang eingeräumt. Beide stehen eigenständig nebeneinander und sind daher gleichermaßen zu berücksichtigen. Dies bedeutet, daß im konkreten Einzelfall festgestellt werden muß, welche Schritte oder Maßnahmen zum technischen Telekommunikationsvorgang gehören und welche zum inhaltlichen Informations- und Kommunikationsangebot.

Dies führt in der praktischen Anwendung des Gesetzes jedoch zu Problemen bei der datenschutzrechtlichen Einordnung der personenbezogenen Daten, die auf der Ebene der Telekommunikation als Verbindungsdaten anfallen. Sie dienen sowohl der technischen Durchführung des Telekommunikationsdienstes und unterfallen insoweit dem bereichsspezifischen Datenschutzrecht in der Telekommunikation. Sie können darüber hinaus aber auch zur Abrechnung bei der Nutzung des Teledienstes von Bedeutung sein, z. B. wenn die Nutzungsentgelte von der Verbindungsdauer zu bestimmten Tageszeiten abhängen. Hierfür wäre das TDDSG einschlägig. Eine eindeutige Differenzierung zwischen dem die „Transportebene“ betreffenden Telekommunikationsrecht und dem „online-Recht“ des TDDSG dürfte bei fortschreitender Entwicklung komplexer Informations- und Kommunikationstechnologien kaum noch durchführbar sein.

Neben dem Problem einer sachgerechten Abgrenzung der einschlägigen Rechtsvorschriften besteht bei der Nutzung eines mittels Telekommunikation durchgeführten Individualdienstes zudem die Schwierigkeit, daß dieser nicht immer eindeutig als Teledienst bzw. als Telekommunikationsdienst eingeordnet werden kann.

So ist es zum Beispiel durchaus fraglich, ob der reine E-Mail-Verkehr ein Telekommunikationsdienst oder auch ein Teledienst ist. Dies gilt insbesondere dann, wenn der Anbieter eines Mailservers zusätzlich zu einer adressierten Nachrichtenpost auch weitere Dienste – z. B. eine Internet-Suchmaschine – anbietet. Die datenschutzrechtliche Einordnung des sog. Access-Providers kann auch davon abhängen, wie sein Kunde das Internet gerade nutzt, was der Provider aus Gründen des Persönlichkeitsrechtsschutzes aber nicht wissen sollte.

Fragen nach Reichweite und Anwendungsbereich von Vorschriften stehen bei neuen Gesetzen häufig im Vordergrund. Um hier praxisgerechte Lösungen zu finden, stehe ich sowohl mit den Landesbeauftragten für den Datenschutz als auch mit den Aufsichtsbehörden für den nicht-öffentlichen Bereich in einem regen Gedankenaustausch und bin zuversichtlich, daß es gelingt, ausreichende Rechtssicherheit für die betroffenen Bürger und Unternehmen zu schaffen. Langfristig dürften die Probleme aber nur durch eine möglichst weitgehende Angleichung der Vorschriften zu lösen sein.

10.1.3 Änderung der TDSV überfällig

Auf der Grundlage von § 10 Abs. 1 PTRegG wurde die TDSV am 12. Juli 1996 von der Bundesregierung mit Zustimmung des Bundesrates als bereichsspezifische Datenschutzverordnung für den Bereich der Telekommunikation verabschiedet. Die TDSV regelt den Schutz der personenbezogenen Daten aller am Fernmeldeverkehr Beteiligten und richtet sich entsprechend den Vorgaben des PTRegG ausschließlich an Unternehmen und Diensteanbieter, die **Telekommunikationsdienstleistungen für die Öffentlichkeit** erbringen oder daran mitwirken.

§ 10 PTRegG ist zum 31. Dezember 1997 außer Kraft getreten und wurde durch § 89 TKG ersetzt. Da Rechtsverordnungen in der Regel auch nach dem Wegfall ihrer gesetzlichen Ermächtigungsgrundlage gültig bleiben, hat die TDSV ihre Rechtskraft nicht verloren und ist weiterhin geltendes Recht. Im Gegensatz zur Vorgängervorschrift gehören nach § 89 Abs. 1 TKG jedoch alle Unternehmen, die **Telekommunikationsdienste geschäftsmäßig** erbringen oder daran mitwirken, zum Adressatenkreis einer bereichsspezifischen Datenschutzverordnung im Bereich der Telekommunikation. Damit werden auch die sog. Corporate Networks, d. h. geschlossene Benutzergruppen von der Verordnung erfaßt. Darunter versteht man – im Gegensatz zu den öffentlichen, für jedermann zugänglichen Telekommunikationsdiensten – Nebenstellenanlagen, wie sie z. B. in Hotels und Krankenhäusern üblich sind, Clubtelefone sowie Nebenstellenanlagen in Betrieben und Behörden, soweit diese den Beschäftigten zur privaten Nutzung zur Verfügung gestellt werden. Für den Kreis der Normadressaten der TDSV scheint sich ein Widerspruch aufzutun. Der ist dahingehend aufzulösen, daß die gesetzliche Vorschrift des § 89 Abs. 1 TKG als höherrangiges Recht der TDSV vorgeht und damit als verbindlicher Auslegungsmaßstab den engen Anwendungsbereich der TDSV erweitert.

Da sich die TDSV auch in einigen anderen Punkten von den Vorgaben des TKG unterscheidet, ist es dringend geboten, diese Wertungswidersprüche im Rahmen einer Änderung der TDSV zu bereinigen. Berücksichtigt man, daß das TKG bereits am 31. Juli 1996 verkündet worden ist, besteht auch unter diesem zeitlichen Aspekt Handlungsbedarf, die TDSV im Sinne der gesetzlichen Vorschrift zu harmonisieren.

Schließlich sollte die Novellierung der TDSV dazu genutzt werden, die einschlägigen Regelungen der EG-Telekommunikations-Datenschutzrichtlinie 97/66/EG vom 15. Dezember 1997 in deutsches Recht umzusetzen. Zwar besitzt Deutschland gerade auch im Bereich der Telekommunikation einen hohen Datenschutzstandard. Gleichwohl sollten die Vorgaben der Richtlinie als Chance betrachtet werden, das nationale Recht des Datenschutzes in der Telekommunikation weiter zu verbessern.

Nach Artikel 15 Abs. 1 der Richtlinie haben die Mitgliedsstaaten der EU die zur Umsetzung der Richtlinie erforderlichen Rechts- und Verwaltungsvorschriften bis zum 24. Oktober 1998 zu erlassen. Diese sehr eng gesetzte Frist konnte von der Bundesregierung zwar nicht eingehalten werden. Erste Überlegungen für eine neue TDSV sind aber bereits mit mir diskutiert worden. Aufgrund dieser Gespräche mit dem insoweit federführenden BMWi gehe ich davon aus, daß noch im Laufe des Jahres 1999 eine neue TDSV in Kraft gesetzt wird.

10.1.4 Schafft die EG-Telekommunikations-Datenschutzrichtlinie neues TK- Recht?

Im Januar 1998 wurde die EG–Telekommunikations-Datenschutzrichtlinie 97/66/EG vom 15. Dezember 1997 veröffentlicht (Abl. Nr. L 24/1 v. 30. Januar 1998 1ff.). Ziel dieser Richtlinie ist es, europaweit ein gleichwertiges Schutzniveau für die Verarbeitung personenbezogener Daten im Zusammenhang mit der Erbringung öffentlich zugänglicher Telekommunikationsdienste zu gewährleisten. Im Anschluß an die allgemeine Datenschutzrichtlinie 95/46/EG aus dem Jahre 1995 ist dies die erste und zugleich eine wichtige bereichsspezifische Datenschutzrichtlinie.

Sie enthält nicht nur allgemeine Regelungen zur Netzsicherheit und zur Vertraulichkeit der Kommunikation, sondern auch spezielle Vorschriften, beispielsweise für die Datenverarbeitung im Zusammenhang mit der Gebührenabrechnung, der Rufnummernanzeige, der Anrufweiterschaltung und der Erstellung von Teilnehmerverzeichnissen.

Die Richtlinie führt nicht dazu, daß es zu einem neuen TK-Recht in Deutschland kommt. Für das TKG sehe ich wegen der Richtlinie zur Zeit keinen Änderungsbedarf. Die nach § 89 TKG ohnehin zu erlassende Nachfolgeverordnung zur TDSV müßte jedoch auch der Richtlinie wegen geändert werden. Dabei handelt es sich nicht um einschneidende Grundsatzregelungen, sondern um Detailprobleme, z. B. im Zusammenhang mit der Rufnummernanzeige und der Anrufweiterschaltung. Wichtig für die Bürger Europas ist allerdings, sich europaweit darauf verlassen zu können, daß gewisse Mindeststandards für den Datenschutz im Bereich der Telekommunikation eingehalten werden.

Die TK-Datenschutzrichtlinie sollte bis zum 24. Oktober 1998 in nationales Recht umgesetzt werden. Wie bei der allgemeinen Datenschutzrichtlinie gilt auch hier, daß der Gesetzgeber in Deutschland die Möglichkeit hat, Regelungen zu treffen, die über den durch die Richtlinie festgesetzten Mindeststandard hinausgehen. Das Bundesministerium für Wirtschaft und Technologie – das als Rechtsnachfolger des BMPT für diesen Bereich zuständig ist – hat die Absicht, dem Kabinett im Frühjahr 1999 den Entwurf für eine neue TDSV vorzulegen; bei Redaktionsschluß lag hierzu ein Referentenentwurf vor.

10.1.5 Datenschutz des Bürgers und Sicherheitsinteressen des Staates – ein Widerspruch?

10.1.5.1 Große Überwachung vorerst gestoppt

Bei der Durchführung der gesetzlich vorgesehenen Maßnahmen zur Überwachung der Telekommunikation stützen sich die hierzu berechtigten Stellen derzeit noch auf die Fernmeldeverkehr-Überwachungs-Verordnung (FÜV) vom 18. Mai 1995. Ermächtigungsgrundlage für diese Verordnung war das inzwischen nicht mehr geltende Fernmeldeanlagengesetz. Mit dem im Juli 1996 in Kraft getretenen TKG ist eine neue Ermächtigungsgrundlage für die technische Umsetzung von Überwachungsmaßnahmen geschaffen worden (§ 88 TKG), die eine umfassende Anpassung der Verordnungsregelung an das neue Telekommunikationsrecht erfordert.

Änderungen ergeben sich zunächst aus der Ausweitung des Adressatenkreises. Im Zuge der vollständigen Aufhebung des staatlichen Fernmeldemonopols durch das TKG ist die Verpflichtung, Abhörmaßnahmen zu ermöglichen, auf alle diejenigen erweitert worden, die geschäftsmäßig Telekommunikationsdienste erbringen oder daran mitwirken, während früher nur die Betreiber **öffentlicher** Telekommunikationsnetze das Abhören ermöglichen mußten. Darüber hinaus sieht § 88 TKG vor, daß die neue Verordnung Vorschriften über die Genehmigung und die Abnahme von Überwachungseinrichtungen sowie über Jahresstatistiken zu Überwachungsmaßnahmen enthalten soll.

Das zuständige BMWi hat als Nachfolgevorschrift für die FÜV nach Maßgabe des § 88 TKG den Entwurf einer Telekommunikations-Überwachungsverordnung (TKÜV) erarbeitet, zu dem vor einer abschließenden Abstimmung innerhalb der Bundesregierung auch den Verbänden, Organisationen und Arbeitsgemeinschaften des Telekommunikationsbereichs Gelegenheit zur Stellungnahme gegeben wurde. Unterstützt durch zahlreiche kritische Presseberichte führten die Äußerungen aus diesem Kreise dazu, daß eine bereits terminierte öffentliche Anhörung abgesagt und der Fortgang des Verordnungsverfahrens vorerst unterbrochen wurde.

Wesentliche Kritikpunkte der in den oben genannten Gremien vertretenen Unternehmen sind vor allem

- die Ausweitung der Verpflichtung zur Bereitstellung von Überwachungsmaßnahmen auf Corporate Networks und Nebenstellenanlagen,
- die Ausdehnung von Überwachungsmaßnahmen auf den E-Mail-Verkehr und die Internet-Telekommunikation sowie

– die unzureichenden Ausnahmeregelungen, z. B. für Nebenstellenanlagen von kleineren Hotels und Pensionen, Firmen, Krankenhäusern und ähnlichen Betrieben.

Nach dem Verordnungsentwurf sollen beispielsweise Betreiber von Nebenstellenanlagen mit mehr als 20 Anschlüssen, die nicht nahezu ausschließlich von eigenem Personal genutzt werden, zur Bereitstellung von Überwachungseinrichtungen verpflichtet werden. Die Einwendungen werden in erster Linie damit begründet, daß die in dem TKÜV-Entwurf vorgesehenen Überwachungsmaßnahmen und -einrichtungen unverhältnismäßig hohe finanzielle Aufwendungen auf Seiten der TK-Unternehmen und -Diensteanbieter zur Folge hätten und die Wettbewerbsfähigkeit deutscher Firmen erheblich beeinträchtigten.

Ich habe darauf hingewiesen, daß der erweiterte Kreis der Verpflichteten sowie die von diesen zu treffenden Maßnahmen durch die Verordnungsregelung konkretisiert und sachgemäß begrenzt werden muß. So habe ich Sorge, daß bei einer Ausdehnung der Verpflichtungen auf Nebenstellenanlagen, insbesondere von Krankenhäusern, aber auch von Zeitungsredaktionen oder großen Anwaltskanzleien, die Wahrung von Berufsgeheimnissen erschwert, wenn nicht unmöglich gemacht wird. Ferner ist – abgesehen davon, daß bei kleineren und mittleren Unternehmen wirtschaftliche Aufwendungen verursacht würden, die in keinem angemessenen Verhältnis zu dem zu erwartenden Nutzen stehen dürften – auch zu befürchten, daß durch die Schaffung einer großen Zahl neuer Überwachungseinrichtungen die Gefahr des Mißbrauchs durch Unbefugte ansteigt.

Außerdem muß die Verordnung sicherstellen, daß Gesprächsinhalte, die wegen ihrer Sensibilität von den Kunden (mit Hilfe des Netzbetreibers) durch Verschlüsselung oder andere technische Maßnahmen besonders geschützt werden, auch bei der Übertragung an die Sicherheitsbehörden mit einem gleichwertigen Schutz versehen werden. Die Zulassung einer ungeschützten Übertragung solcher Gespräche von der Abhörschnittstelle beim Verpflichteten – möglicherweise quer durch ganz Deutschland – bis zur Sicherheitsbehörde, die die Überwachungsmaßnahme durchführt, wäre aus meiner Sicht nicht hinnehmbar.

Bei Redaktionsschluß lag noch kein überarbeiteter Entwurf der TKÜV vor. Ich hoffe, daß die neue Bundesregierung meinen Bedenken Rechnung tragen wird.

10.1.5.2 Wissensdurst des Staates nimmt zu: Standortbestimmung von Mobiltelefonen

Ende 1997 erschienen erste Presseberichte, in denen von der Standortbestimmung von Mobiltelefonen für Sicherheitsbehörden berichtet wurde. Danach könne eine Firma in der Schweiz über ihr Mobilfunknetz den Aufenthaltsort ihrer Kunden rückwirkend bis zu einem Jahr feststellen. Diese Berichterstattung sorgte dann auch für viel Diskussionsstoff und eine Reihe von Fragen in Deutschland.

Im Laufe des Jahres 1998 gab es dann in Deutschland gerichtliche Beschlüsse, über die auch in der Presse berichtet wurde. Durch diese Beschlüsse wurden Mobilfunkunternehmen dazu verpflichtet, Sicherheitsbehörden die Standorte von Mobiltelefonen auch dann mitzuteilen, wenn nicht telefoniert wird, sondern sich das Handy nur im sog. Stand-by-Modus befindet. In dieser Situation setzt sich das Handy in bestimmten Zeitabständen selbständig mit dem Netz in Verbindung. Dabei erfährt das Netz u. a. auch die Funkzelle – also den ungefähren Aufenthaltsort –, in der sich das Handy gerade befindet. Diese Kommunikation geschieht vollautomatisch und ohne daß dies im Regelfall vom Benutzer bemerkt wird. Sie dient vor allem dazu, daß das Netz weiß, wo das Mobiltelefon sich befindet und einen ankommenden Anruf dort hinleiten kann.

Ich habe hierzu darauf hingewiesen, daß nach der geltenden Rechtslage die Mitteilung der Funkzelle an eine Sicherheitsbehörde nur im Rahmen einer richterlich angeordneten Überwachungsmaßnahme zulässig ist und auch nur, wenn tatsächlich ein Gespräch stattfindet. In diesem Fall ist der Sicherheitsbehörde gemäß § 3 Abs. 2 Nr. 4 FÜV auch die Funkzelle mitzuteilen, über die die Verbindung abgewickelt wird. Es war von Seiten des Gesetzgebers auch nicht beabsichtigt, diese Möglichkeit als zulässige Maßnahme der Strafverfolgungsbehörden auf die Fälle auszuweiten, in denen das Handy nur im Stand-by-Modus ist. Dies wurde im Rahmen des Gesetzgebungsverfahrens zum TKG-Begleitgesetz Ende 1997 deutlich (s. auch Nr. 10.1.1). Die Bundesregierung hat seinerzeit festgestellt, daß von gesetzgeberischen Regelungsvorschlägen zur Erfassung von Aufenthaltsdaten abgesehen wurde, weil das praktische Bedürfnis der Sicherheitsbehörden für die Erfassung der Daten aufgrund der Aktivmeldungen des Handy besonders deutlich nachzuweisen sei. Dieser Nachweis sei von ihnen aber bisher nicht erbracht worden.

Die Diskussionen in der Öffentlichkeit habe ich zum Anlaß genommen, mich bei den großen Betreibern von Mobilfunknetzen zu erkundigen, ob und inwieweit Standortmeldungen in ihrem System gespeichert werden. Es wurde mir bestätigt, daß im Stand-by-Modus nur die aktuelle „Location Area“ kurzfristig zwischengespeichert wird, um dem Handy so Gespräche überhaupt zuleiten zu können. Eine Speicherung der Funkzellen je Handy über einen längeren Zeitraum ist im System nicht vorgesehen.

Während ein Kunde mit seinem Handy telefoniert, wird die Funkzellenkennung gespeichert und zu Abrechnungszwecken als Teil der Verbindungsdaten gespeichert. Bei Wechsel der Funkzelle während des Gesprächs wird nur die Zelle gespeichert, in der das Gespräch begonnen hat. Wegen der Regelungen in der TDSV darf die Speicherung in diesem Fall höchstens 80 Tage andauern, falls der Kunde sich für die Option der Speicherung seiner Daten nach Rechnungsversand entschieden hat. Eine Mitteilung von Standortdaten nach einem Jahr – wie von der Schweiz berichtet – ist in Deutschland demnach nicht nur rechtlich unzulässig, sondern technisch auch nicht vorgesehen.

10.1.5.3 Auskünfte an die Sicherheitsbehörden über Kundendaten: Neue Begehrlichkeiten des Staates?

Gleich zwei Vorschriften des TKG eröffnen staatlichen Stellen die Möglichkeit, Informationen über die Kunden von TK-Unternehmen zu erlangen:

So müssen TK-Unternehmen nach **§ 90 TKG** eine Kundendatei führen, in die Rufnummern bzw. Rufnummernkontingente sowie Name und Anschrift der Inhaber der Rufnummern bzw. Rufnummernkontingente aufzunehmen sind. Das gilt auch, soweit die Kunden in öffentlichen Verzeichnissen nicht eingetragen sind. Die aktuellen Kundendateien sind so verfügbar zu halten, daß die Regulierungsbehörde für Telekommunikation und Post (RegTP) einzelne Daten oder Datensätze in einem von ihr vorgegebenen automatisierten Verfahren abrufen kann. Die RegTP hat die Daten auf Ersuchen der in § 90 genannten auskunftsberechtigten Sicherheitsbehörden automatisiert abzurufen und an die ersuchende Stelle zu übermitteln.

Mit dieser Vorschrift wollte der Gesetzgeber dem Umstand Rechnung tragen, daß – anders als früher – Auskunftsersuchen über die genannten Daten nicht mehr nur von einer Stelle, der Telekom, beantwortet werden können, sondern hierfür nach der vollständigen Liberalisierung des Telekommunikationsmarktes zahlreiche TK-Unternehmen und -Diensteanbieter als Adressaten in Frage kommen. Um zeitraubende Recherchen darüber, bei wem diese Daten gespeichert sind, zu vermeiden, wurde die Rechtsgrundlage für ein automatisiertes Abrufverfahren geschaffen.

Die Vorschrift ist bereits vor ihrem Inkrafttreten heftig diskutiert worden (siehe hierzu 16. TB Nr. 10.1.5). Inzwischen haben sich die Befürchtungen bewahrheitet, daß die Regelung des § 90 TKG weit über das angestrebte Ziel hinausschießt, da nach ihr jeder verpflichtet ist, *„der geschäftsmäßig Telekommunikationsdienste anbietet."*

Seitens der Bundesregierung wurde auf eine parlamentarische Anfrage mitgeteilt (Drucksache 13/11329, S. 25), daß nach Untersuchungen der RegTP von der Vorschrift *„nach derzeitiger Rechtslage ca. 400 000 Unternehmen betroffen (wären). ... Deshalb soll in der ersten Ausbauphase zunächst mit Anbietern von Telekommunikationsdiensten begonnen werden, die eine Lizenz nach der Lizenzklasse 1 oder 4 des TKG erhalten haben. Es handelt sich hierbei um 72 Unternehmen."* Das BMWi hat mir auf Anfrage mitgeteilt, daß darüber, *„wann und unter welchen Bedingungen der zahlenmäßig große Bereich derjenigen in das Verfahren einbezogen werden kann, die Telekommunikationsdienste in dem Rahmen anbieten, der früher mit dem Begriff „Nebenstellenanlage" bezeichnet wurde,"* erst dann entschieden werden könne, wenn ausreichende Erfahrungen mit dem Verfahren vorlägen.

Allerdings hat das BMWi bekräftigt, daß die Verpflichtungen des § 90 TKG grundsätzlich auch sämtliche Betreiber von Nebenstellenanlagen treffen, die ihre Anschlüsse Dritten geschäftsmäßig (unabhängig von einer Gewinnerzielungsabsicht) zur Verfügung stellen. Dies gelte ausnahmslos, so daß z. B. auch Krankenhäuser, die ihren Patienten Telefone zur persönlichen Nutzung zur Verfügung stellen, entsprechende Kundendateien zu führen haben.

Nach dieser Stellungnahme ist in absehbarer Zeit nicht damit zu rechnen, daß Nebenstellenanlagen in das Verfahren nach § 90 TKG einbezogen werden. Umso wichtiger ist es, vor einer Ausweitung des Verfahrens auf weitere als die vom BMWi gezählten 72 Unternehmen eine rechtliche Klarstellung herbeizuführen. Ich habe bereits frühzeitig Bedenken gegen eine undifferenzierte, weite Festlegung des Kreises der Verpflichteten angemeldet. Als fraglich sehe ich es insbesondere an, ob § 90 TKG eine hinreichend normenklare Rechtsgrundlage z. B. für die Durchbrechung der ärztlichen Schweigepflicht darstellt oder ob Krankenhäuser und gegebenenfalls auch Nebenstellenanlagen in Bereichen, in denen andere Berufsgeheimnisse berührt sind, vom Geltungsbereich des § 90 TKG ausgenommen werden müssen. Wirtschaftlich kaum vertretbar ist es auch, z. B. von einem Handwerksbetrieb mit 20 Telefonen die Installation des teuren „§ 90-Auskunftscomputers" zu verlangen. Ich habe dem BMWi mitgeteilt, daß ich eine Änderung der Vorschrift begrüßen würde. Aus seinen Ausführungen zur derzeitigen Rechtslage (vgl. oben) entnehme ich, daß eine solche Änderung auch von seiten der Bundesregierung für möglich angesehen wird.

Ein weiteres gravierendes Problem des § 90 TKG ist, daß staatlichen Stellen bei Anfragen nicht nur die Daten der Personen bekannt werden könnten, nach denen sie tatsächlich suchen, sondern möglicherweise auch die Daten Unbeteiligter, nämlich dann, wenn Anfragen mit unvollständigen Rufnummern oder unvollständigen Namens- bzw. Adressangaben getätigt werden („Jokerabfragen", so genannt wegen der als Füllzeichen eingesetzten „Jokerzeichen" ✱ und **?**, z. B. „0228/81995**? ?**" oder „0228/819✱").

Die Sicherheitsbehörden haben Abfragemöglichkeiten mit unvollständigen Daten als unerläßlich bezeichnet, weil ihnen im Rahmen ihrer Ermittlungen oftmals nur schlecht leserliche oder unvollständige Angaben zur Verfügung stünden; dies erscheint plausibel. Ich habe gegenüber der Bundesregierung jedoch betont, daß das TKG solche uneindeutigen Abfragen nicht zuläßt. Hierzu fehlt eine gesetzliche Ermächtigung, die geschaffen werden müßte. In dieser gesetzlichen Ermächtigung müßten genaue Voraussetzungen für Jokerabfragen festgelegt werden. Sie müssen auf das Unerläßliche der in § 90 TKG genannten Zwecke beschränkt werden. Ausgeschlossen werden müßten Abfragen, mit denen bei geschickter Verwendung des Jokerzeichens z. B. die nahezu komplette Belegschaftsliste einer Firma herausgegeben wird (nämlich sämtliche Inhaber der dem Firmenanschluß nachgeordneten Nebenstellen) oder beispielsweise sämtliche Personen, die aktuell in einem Krankenhaus ein Telefon gemietet haben. Aufgrund der von mir vorgebrachten Bedenken zur fehlenden Rechtsgrundlage, die von einigen Bundesministerien geteilt werden, wird die RegTP „Jokerabfragen" erst zulassen, nachdem hierzu eine tragfähige Rechtsgrundlage geschaffen worden ist.

Nach **§ 89 Abs. 6 TKG** müssen den Sicherheitsbehörden, wenn dies zur Erfüllung ihrer Aufgaben (u. a. Gefahrenabwehr und Verfolgung von Straftaten und Ordnungswidrigkeiten) erforderlich ist, im Einzelfall von den TK-Unternehmen die **Bestandsdaten** ihrer Kunden mitgeteilt werden (Name, Anschrift, Telefonnummer usw.). Die **Verbindungsdaten** sind – wie in der amtlichen Begründung zu § 89 TKG ausdrücklich klargestellt wird – von diesem Auskunftsanspruch nicht betroffen.

Zwar hat der Gesetzgeber bei der Ausgestaltung der Vorschrift des § 89 Abs. 6 TKG über die Auskunftspflicht der TK-Unternehmen eine Ausnahme vom datenschutzrechtlichen Zweckbindungsgrundsatz geschaffen. Entsprechend dem datenschutzrechtlichen Prinzip, Daten nur zu dem Zweck zu verwenden, zu dem sie auch erhoben worden sind, muß § 89 Abs. 6 TKG aber einschränkend ausgelegt werden. Die Notwendigkeit für eine einschränkende Auslegung wurde dadurch deutlich, daß die Vorschrift übermäßig ausgedehnt wurde:

Sämtliche Daten, die ein Unternehmen bei Vertragsabschluß von dem Kunden erhoben hat, wurden abgefordert.

Der Auskunftsanspruch muß deshalb streng auf solche Daten beschränkt werden, die einen besonderen Telekommunikationsbezug haben, wie z. B. der Name des Anschlußinhabers, der Standort und die Rufnummer des Anschlusses. Die Preisgabe weiterer Daten, wie z. B. der Bankverbindung des Anschlußinhabers oder der Zugehörigkeit zu bestimmten gesellschaftlichen Gruppen, denen Sondertarife eingeräumt werden, darf den TK-Unternehmen aufgrund § 89 Abs. 6 TKG nicht abverlangt werden. Ein Anspruch, in einem „vereinfachten Verfahren" über die telekommunikationsspezifischen Daten hinausgehende beliebige Kundendaten zu erhalten, den es in anderen Branchen der Privatwirtschaft nicht gibt, läßt sich auch für den TK-Bereich nicht rechtfertigen. Auskunftersuchen über nicht telekommunikationsspezifische Daten können daher nicht auf das TKG gestützt werden, sondern nur auf die einschlägigen Vorschriften, etwa der StPO, sofern die Voraussetzungen dafür im Einzelfall vorliegen.

10.1.6 Ausreichender TK-Datenschutz durch einen „Katalog von Sicherheitsanforderungen"?

Nach § 87 Abs. 1 TKG haben alle TK-Unternehmen beim Betrieb ihrer Telekommunikations- und Datenverarbeitungssysteme *„angemessene technische Vorkehrungen oder sonstige Maßnahmen zum Schutze ... des Fernmeldegeheimnisses und personenenbezogener Daten ... zu treffen."*

Ich habe mich im Gesetzgebungsverfahren sehr für eine solche explizite rechtliche Verpflichtung der TK-Unternehmen eingesetzt, denn bis heute führen Sicherheitsmängel bei der eingesetzten Technik zu Verärgerung, oft aber auch zur Verletzung der Datenschutzrechte der Kunden. In der Vergangenheit waren dies etwa mangelhafte, unverantwortliche Leitungsführungen der Telefonanschlußleitung. Wurde diese – wie häufig geschehen – durch den Keller eines Nachbarhauses geführt, konnte sie – jedenfalls im Falle von Streitigkeiten – auch schon mal eine Einladung zur „privaten Telefonüberwachung" bedeuten.

Heute zeigen sich Sicherheitsmängel häufiger in der komplexen Software der eingesetzten IT-Systeme. So führte erst kürzlich ein solcher Fehler dazu, daß über tausend Telefonkunden ihre **Einzelverbindungsnachweise** nicht erhielten. Der wurde stattdessen – in Form mehrerer, dikker Pakete – einer Handvoll anderen Kunden zugestellt, was auch ein größeres Presseecho zur Folge hatte; zum Glück waren dabei die Namen der betroffenen Anschlußinhaber „technisch verlorengegangen".

Die Erfüllung der genannten Verpflichtung kann gemäß § 87 Abs. 3 TKG durch Rechtsverordnung geregelt werden. Das frühere BMPT erklärte seinerzeit hierzu, von dieser Verordnungsermächtigung solange keinen Gebrauch machen zu wollen, wie TK-Unternehmen aus eigenem Antrieb ausreichende Schutzmaßnahmen ergreifen. Dabei soll ihnen ein „Katalog von Sicherheitsanforderungen" Hilfestellung leisten. Den soll gemäß § 87 Abs. 1 TKG die Regulierungsbehörde für Telekommunikation und Post im Benehmen mit dem BSI erstellen, *„um eine nach dem Stand der Technik und internationalen Maßstäben angemessene Standardsicherheit zu erreichen. Dem Bundesbeauftragten für den Datenschutz ist Gelegenheit zur Stellungnahme zu geben."*

In meiner Stellungnahme habe ich nachdrücklich darauf hingewiesen, daß – angesichts des Fehlens einer Rechtsverordnung – dem „Katalog von Sicherheitsanforderungen" besondere Bedeutung als *„Meßlatte für die Sicherheit in der Telekommunikation"* zukommt (s. 16. TB Nr. 10.2.2). Er muß den TK-Unternehmen klar erkennbare und erfüllbare, aber auch ausreichende und angemessene Vorgaben für die Sicherheit der Telekommunikationsdienste machen. Der Katalog muß einem TK-Unternehmen ermöglichen, die für seinen Dienst relevanten Sicherheitsanforderungen zweifelsfrei zu erkennen und deren jeweilige Bedeutung – für den zu betreibenden Aufwand – einzuschätzen. Darüber hinaus muß er dem TK-Unternehmen möglichst auch Empfehlungen für solche Maßnahmen geben, durch die eine vom Gesetzgeber geforderte *„angemessene Standardsicherheit"* zu erreichen ist.

Dies leistet der Katalog nur ansatzweise; er bedarf daher einer konzeptionellen und inhaltlichen Überarbeitung. Unerläßlich ist insbesondere eine Ergänzung hinsichtlich system- und organisationsbezogener Anforderungen, die von den eingesetzten Anlagen und Systemen zu erfüllen sind. Wegen der durch die zögerliche Erarbeitung des Kataloges eingetretenen zeitlichen Enge habe ich mich seinerzeit mit dem BMPT darauf verständigt, daß meine Änderungsvorschläge und Anregungen erst bei der Überarbeitung des Katalogs vor dem Hintergrund der dann gewonnenen Erfahrungen einbezogen werden. Eine frühzeitige Beteiligung bei der Überarbeitung wurde mir von der Regulierungsbehörde für Telekommunikation und Post zugesagt.

Der „Katalog von Sicherheitsanforderungen" ist als Beilage Nr. 208a aus 1997 im Bundesanzeiger veröffentlicht.

10.1.7 Zusammenarbeit mit der Regulierungsbehörde

Im Januar 1998 hat die Regulierungsbehörde für Telekommunikation und Post (RegTP) ihre Tätigkeit aufgenommen. Rechtsgrundlage für ihre Errichtung ist das TKG (§ 66). Die RegTP hat die Aufgabe, die Einhaltung der Vorschriften des TKG zu überwachen. Ziel ist es u. a., durch Regulierung den Wettbewerb zu fördern und flächendeckend angemessene und ausreichende Dienstleistungen zu gewährleisten. Zu den insoweit wichtigen Aufgaben gehören z. B. die Lizenzerteilung an neue Unternehmen und die Entgeltregulierung.

Die RegTP hat aber auch Aufgaben zur Kontrolle und Durchsetzung von Verpflichtungen der TK-Unternehmen wahrzunehmen (§ 91 TKG). Hierzu kann sie Anordnungen und Maßnahmen treffen, um die Einhaltung der Vorschriften des Elften Teils des TKG sicherzustellen; dazu gehören auch solche über das Fernmeldegeheimnis (§ 85) und den Datenschutz (§ 89). Um Verpflichtungen der TK-Unternehmen in diesem Bereich durchzusetzen, kann die Regulierungsbehörde auch Kontrollen vornehmen, aber auch Zwangsgelder festsetzen oder das geschäftsmäßige Erbringen des Telekommunikationsdienstes ganz oder teilweise untersagen.

Die Zuständigkeit für Kontrollen im Bereich des Datenschutzes wurde – abweichend von § 38 BDSG – anstelle der Aufsichtsbehörden der Länder mir zugewiesen (§ 91 Abs. 4 TKG). Dadurch kommt es zu einer gewissen „Doppelzuständigkeit“ für die RegTP und mich.

Um sicherzustellen, daß die Datenschutzvorschriften eingehalten werden und um die Aufgabenerfüllung zu koordinieren, habe ich mich von Anfang an für eine enge Zusammenarbeit mit der Regulierungsbehörde eingesetzt. Seit dem Frühjahr 1998 finden dazu regelmäßig Gespräche in Form eines „Jour Fixe“ zwischen meinem Haus und der RegTP statt.

10.1.8 Datenarme Telekommunikation

Waren- und Dienstleistungsangebote sollten so gestaltet sein, wie es der Kunde wünscht. Daß dies stimmt, weiß leider noch nicht jeder Anbieter von Telekommunikationsdiensten: Jahrzehntelang mußte der Bürger z. B. das Telefonmodell hinnehmen, das ihm die Post „überließ“, wie es damals vielsagend hieß. Entsprechendes galt für die (hohen) Preise; beides behinderte Akzeptanz und Verbreitung der Telekommunikation. Einig sind sich die Nutzer vor allem in zwei Forderungen:

Geringe Kosten und hoher Schutz der Vertraulichkeit der Nachrichten.

Weder das TK-Unternehmen noch einen Dritten geht es etwas an, worüber im Telefonat oder per Fax kommuniziert wurde.

Unterschiedliche Bewertungen gibt es darüber, welche Daten zu den „näheren Umständen“ der Telekommunikation gehören, wie z. B. die Anzeige der Rufnummer des Anrufers beim Angerufenen (s. u. Nr. 10.2.8). So ist es Eltern sicherlich recht, daß die angerufenen Kinder ihre Rufnummer erkennen können – und damit den Anruf entgegennehmen. Rufen die gleichen Eltern bei verschiedenen Öllieferanten an, um den günstigsten Heizölpreis zu erfragen, wird ihnen die Rufnummeranzeige wegen des Risikos späterer Werbeanrufe eher nicht recht sein. Hier gehen wie so oft die Forderungen des Datenschutzes in dieselbe Richtung wie die Verbraucherwünsche und gerade bei der Gestaltung neuer TK-Dienstleistungen müssen beide Aspekte berücksichtigt werden. So muß die Möglichkeit einer detailreichen Registrierung des Telekommunikationsvorganges genauso gegeben sein wie die Möglichkeit der anonymen Kommunikation. Diese Forderung für die Gestaltung neuer TK-Dienstleistungen ist inzwischen in der Gesellschaft und im politischen Raum allgemein akzeptiert (s. o. Nr. 8.5).

Diejenigen, die TK-Dienstleistungen konzipieren, scheinen aber immer wieder zu vergessen, daß ihre Systeme die Kundenwünsche berücksichtigen sollten. Typisch hierfür ist die Datenstruktur der **GSM-Telefonnetze** (D1-, D2- und ePlus-Netz): Bei ihrer Konzeption wurde eine selbst von Experten kaum übersehbare Fülle von Datenspeicherungen („Vielleicht brauchen wir sie ja ’mal ...“) vorgesehen, von denen viele bis heute nicht benötigt werden. Anonyme oder pseudonyme Nutzungsmöglichkeiten wurden nicht vorgesehen und erst später „hineingeflickt“. So gibt es bis heute in den Mobilfunknetzen keine Tarife, die tatsächlich von der Entfernung der beiden Kommunikationspartner abhängig sind; gleichwohl wird der Standort des Handy beim Gesprächsbeginn registriert.

Auch für die Telekommunikation wird die Schaffung und der Einsatz datenschutzfreundlicher und datenarmer Technologien allgemein für erforderlich gehalten. Bei meiner Beratungs- und Kontrolltätigkeit habe ich hierzu jedoch sowohl in den zuständigen Bundesministerien als auch den TK-Unternehmen deutliche Informationslücken dazu festgestellt, wie solche Technologien denn auszusehen hätten. So ist es auch erklärlich, daß mögliche Strategien für eine Problemlösung bislang nicht entwikkelt wurden.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat in ihrem Arbeitskreis „Technische und organisatorische Datenschutzfragen“ einen Versuch unternommen, hier den für den Datenschutz in der öffentlichen Verwaltung und der Privatwirtschaft Verantwortlichen Anstöße und Hilfen für die Entwicklung entsprechender Konzepte zu geben. Sein Arbeitspapier „Datenschutzfreundliche Technologien in der Telekommunikation“ – der vollständige Text kann unter meiner Homepage http://www.bfd.bund.de aufgerufen werden – enthält neben einer Problemdarstellung auch Ansätze für die Datenvermeidung und –reduzierung bei der Entwicklung neuer TK-Dienste. Das Arbeitspapier enthält auch Darstellungen der wichtigsten TK-Systeme, so auch der GSM-Mobilfunknetze und des ISDN. Seit dem Erscheinen des Arbeitspapiers Ende 1997 habe ich es vielen Interessenten auf ihre Bitte hin – auch in elektronischer Form, nämlich per E-Mail – zugesandt. Ich werde daher darauf hinwirken, daß es in angemessenen Zeitabständen aktualisiert und fortgeschrieben wird.

10.1.9 Datenschutz jetzt auch für die Nutzer von Telefonanlagen

Aus dem Verhältnis zwischen dem – im August 1996 in Kraft getretenen – TKG und der bereits seit Juli 1996 geltenden Telekommunikationsdienstunternehmen-Datenschutzverordnung (TDSV) ergibt sich eine Änderung der Rechtslage auch für die Betreiber von TK-Anlagen, früher Telefon-Nebenstellenanlagen genannt. Die TDSV gilt nämlich ihrem Wortlaut nach nur für Unternehmen und Diensteanbieter, die der **Öffentlichkeit angebotene TK-Dienstleistungen** erbringen. Die Vorschriften des Elften Teils des TKG (Fernmeldegeheimnis, Datenschutz, Sicherung) – insbesondere § 89 TKG (Datenschutz) – richten sich jedoch an Personen und Unternehmen, die **geschäftsmäßig Telekommunikationsdienste** erbringen. Dies sind alle, die ein auf Dauer angelegtes Angebot von TK-Diensten vorhalten. Unerheblich ist dabei, ob es sich an die Öffentlichkeit oder nur an bestimmte Kunden richtet und ob damit eine Gewinnerzielungsabsicht verbunden ist (§ 3 Nr. 5 TKG). Die datenschutzrechtlichen Vorschriften des § 89 TKG sowie der auf sie gestützten Rechtsverordnung, nämlich der TDSV, sind deshalb nicht nur auf TK-Dienste, die der Öffentlichkeit angeboten werden, anzuwenden, sondern auch auf solche für „geschlossene Benutzergruppen“. Dies sind neben sog. Corporate Networks (d. h. landesweite Netzwerke von Unternehmen oder Behörden; s. o. Nr. 10.1.3) auch TK-Anlagen in Firmen und Hotels, soweit sie den Beschäftigten, Gästen usw. auch zur privaten Nutzung zur Verfügung gestellt werden.

Mit Schreiben vom 3. Juli 1997 (s. **Anlage 21**) habe ich die obersten Bundesbehörden auf die veränderte Rechtslage aufmerksam gemacht.

Gleichzeitig habe ich mich mit gleichlautendem Schreiben (s. **Anlage 22**) an die Spitzenverbände aus Industrie und Wirtschaft mit der Bitte um entsprechende Information ihrer Mitglieder gewandt. Mein Angebot zur Beratung ist von einigen dieser Adressaten inzwischen angenommen worden.

In meiner Informationsbroschüre „BfD-Info 5 Datenschutz und Telekommunikation“ sind darüber hinaus Auszüge aus Empfehlungen zum Datenschutz in der Telekommunikation abgedruckt, die ich vor Inkrafttreten des TKG gegenüber den öffentlichen Stellen des Bundes abgegeben habe. Auch aus ihnen lassen sich Anregungen für die Gestaltung und den Betrieb von TK-Anlagen entnehmen. Die Broschüre ist auch in meinem Internet-Angebot enthalten (http://www.bfd.bund.de).

10.2 Der Markt legt Datenschutzproblem offen

10.2.1 „Wo gehobelt wird, da fallen Späne“ – auch in der Telekommunikation?

Wer heute einen Telefonanschluß bei einem TK-Unternehmen beantragt, hat in diesem Zusammenhang „die Qual der Wahl“. So kann er bestimmen, wie die *Verbindungsdaten*, die bei jedem der von seinem Anschluß ausgehenden Gespräche anfallen, gespeichert werden (Vollspeicherung der Zielrufnummer, Verkürzung oder sofortige Löschung). Er kann bestimmen, ob seine *Rufnummer* beim Angerufenen in jedem Fall oder nur fallweise oder auch nie angezeigt werden soll. Er kann auch festlegen, wie sein Anschluß in öffentliche *Kundenverzeichnisse* (z. B. Telefonbücher, CD-ROM) aufgenommen werden soll (überhaupt nicht oder nur mit seinem Namen oder mit Namen und vollständiger Adresse oder nur mit verkürzter Adresse usw.) oder welche *Auskünfte* über seinen Anschluß erteilt werden dürfen.

Diese und weitere Wahlmöglichkeiten bieten sich aber auch jedem, der bereits über einen Telefonanschluß verfügt. Meist genügt hierfür ein kurzer Anruf beim Diensteanbieter.

Auch um die entsprechenden Wünsche der Kunden erfüllen zu können, werden ihre Daten in Datenbanksystemen geführt, in denen die Daten in vielfältiger Weise miteinander verknüpft sind. Viele Mitarbeiter der TK-Unternehmen sind damit beschäftigt, die Daten entsprechend den Kundenwünschen auf einem aktuellen Stand zu halten. Oft gehen täglich tausende der verschiedensten Kundenwünsche bei den Diensteanbietern ein, die nicht zuletzt aus Wettbewerbsgründen schnell bearbeitet werden sollen.

Wie ich mich überzeugen konnte, ist dies ein oft von Hektik geprägtes Massengeschäft. Das Besondere dieses Geschäfts besteht aber darin, daß dabei – in jedem einzelnen Fall – mit personenbezogenen Daten umgegangen wird. Welche – manchmal auch tragischen – Konsequenzen dabei aus der Fehlhandlung eines einzelnen Bearbeiters oder ungünstig gestalteten Arbeitsabläufen für die davon Betroffenen erwachsen können, zeigen einige Beispiele, die ich nachfolgend unter Nr. 10.3.2 beschrieben habe.

Bei meinen Beratungen und Kontrollen von TK-Unternehmen wird von deren Mitarbeitern – auch solchen in leitenden Funktionen – das Argument, daß die Bearbeitung von Kundenwünschen ein Massengeschäft sei, gern als vorweggenommene Entschuldigung für einzelne Arbeitsfehler vorgebracht. Aus Datenschutzsicht kann ich dieses Verhalten nicht teilen. Gerade das Wissen darum, daß ein bestimmter Arbeitsvorgang jedenfalls zeitweilig in sehr großer Anzahl auftreten kann, verpflichtet eine datenverarbeitende Stelle zu diesbezüglichen sicherheitserhöhenden technischen und organisatorischen Maßnahmen!

Ich appelliere an alle TK-Unternehmen, ihre Mitarbeiter so zu sensibilisieren und zu schulen, daß gerade auch bei der Bearbeitung massenhaft auftretender Geschäftsanfälle, bei denen mit personenbezogenen Daten umgegangen wird, höchste Aufmerksamkeit und Sorgfalt geboten ist. Ich empfehle, Arbeitsfehler regelmäßig und unternehmensweit auszuwerten, um den Mitarbeitern auch die Konsequenzen aus ihren Fehlern aufzuzeigen.

10.2.2 Prepaid-Cards im Mobilfunk

Das Bezahlen von Waren und Dienstleistungen mittels elektronischer Zahlungssysteme gewinnt in allen Lebensbereichen zunehmend an Bedeutung. Von der

Kreditwirtschaft wird derzeit ganz besonders das Bezahlen mit der „Geldkarte“, der ec-Karte mit „aufgeladenem“ Chip, gefördert (vgl. 16. TB Nr. 9.3.2). So ist es seit einiger Zeit auch möglich, mit dem Handy per vorausbezahlter Chipkarte (Prepaid-Card) zu telefonieren. Beim Prepaid-Verfahren stellt die Chipkarte eine aufladbare Guthabenkarte dar. Wie auch bei der bekannten Telefonkarte der DTAG wird bei jeder Nutzung ein entsprechender Betrag vom vorausbezahlten Guthaben abgebucht, bis dieses verbraucht ist.

Ein datenschutzrechtlicher Grundsatz ist es, daß nur Daten erhoben und verarbeitet werden dürfen, soweit dies erforderlich ist. Im Zusammenhang mit dem Verkauf der Prepaid-Cards ergibt sich somit die Frage, ob das jeweilige TK-Unternehmen hier überhaupt Kundendaten speichern darf und wenn ja, welche. Denn nachdem der Käufer das Guthaben vorausbezahlt hat, ist kaum vorstellbar, wozu das TK-Unternehmen noch Daten des Käufers braucht.

Ein von mir kontrolliertes Unternehmen speicherte bis Ende 1998 bei Prepaid-Cards folgende **Bestandsdaten**:

Name, Vorname, Geburtsdatum, Anschrift, Familienstand, Staatsangehörigkeit und Telefonnummer des Kunden.

Zugleich wurde die Vorlage eines amtlichen Ausweises verlangt. Auf meinen Einwand hin werden nunmehr keine Angaben mehr zum Familienstand und zur Staatsangehörigkeit verlangt; auf die Vorlage eines amtlichen Ausweises wird verzichtet. Im übrigen werden das Geburtsdatum und die Telefonnummer im Auftragsvordruck als freiwillige Angaben gekennzeichnet.

Aus Sicht des betreffenden Unternehmens ist die Erhebung von Bestandsdaten beim Verkauf von Prepaid-Cards weder für die Begründung des Vertragsverhältnisses noch für die Erbringung des Dienstes erforderlich. Sie werden lediglich erhoben und gespeichert, vom Unternehmen jedoch weder genutzt noch dafür vorgesehen. Nach den Darlegungen des Unternehmens verursachen die Erhebung sowie die nachfolgende automatisierte Verarbeitung nicht nur erheblichen Aufwand und Kosten, sondern sie behindern auch die Vermarktung des Produktes. Mangels Erforderlichkeit sind die **Erhebung von Bestandsdaten** für die Begründung des Vertragsverhältnisses und die Erbringung des Dienstes beim Verkauf von Prepaid-Cards somit als **unzulässig** anzusehen.

Zur Frage der Zulässigkeit einer solchen Datenerhebung hat das betreffende Unternehmen jedoch auf die vom ehemaligen BMPT erteilte lizenzrechtliche Genehmigung verwiesen, die unter der Auflage erfolgte, *„daß die Ermöglichung von Überwachungsmaßnahmen nach den gesetzlichen Bestimmungen gegeben sein muß .... Der Kunde muß beim Erwerb der ...-Card seine wesentlichen Identifizierungsmerkmale angeben, so daß es sich um ein individualisiertes Kundenverhältnis handelt.“* Die Frage, ob die Lizenzerteilung mit einer solchen Auflage versehen werden durfte, liegt außerhalb meiner Zuständigkeit.

Die Problematik habe ich im Herbst 1998 zum Anlaß genommen, sie mit dem jetzt zuständigen BMWi zu diskutieren. In der mir hierzu vorliegenden Stellungnahme hat mir das BMWi u. a. mitgeteilt, daß sich die Pflicht zur Erhebung von Kundendaten aus § 90 Abs. 1 TKG ergebe. Danach sei jeder geschäftmäßige Anbieter von Telekommunikationsdiensten verpflichtet, Kundendateien zu führen, in die unverzüglich die Rufnummer und Rufnummernkontingente, die zur weiteren Vermarktung oder sonstigen Nutzung an andere vergeben werden, sowie Name und Anschrift der Inhaber von Rufnummern und Rufnummernkontingenten aufzunehmen seien. Die Bestimmungen der §§ 89 und 90 TKG seien selbständige Rechtsverpflichtungen, die nebeneinander bestünden. Es sei nicht erkennbar, daß sich die Verpflichtung aus § 90 TKG nur auf die Daten beziehe, die der Diensteanbieter aufgrund des § 89 TKG in Verbindung mit der TDSV erhoben habe.

Aus den dargelegten Gründen sieht das BMWi keine Möglichkeit, die Anbieter von Produkten, die wie ...-Card oder vergleichbar gestaltet sind, von der Verpflichtung des § 90 TKG auszunehmen.

Die vom BMWi eingenommene Haltung ist aus meiner Sicht **nicht** befriedigend. Entscheidend für die datenschutzpolitische Bewertung der Angelegenheit ist vor allem die von verschiedenen Stellen wiederholt erhobene Forderung, zur Förderung der Akzeptanz neuer Anwendungen der Informationstechnik auch **anonyme Nutzungsmöglichkeiten** vorzusehen. Die 54. Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat am 23./24. Oktober 1997 einen entsprechenden Beschluß gefaßt (s. o. Nr. 8.5). In diesem Zusammenhang ist auch der Schlußbericht der Enquete-Kommission „Zukunft der Medien in Wirtschaft und Verwaltung“ des Deutschen Bundestages zu erwähnen, in dem *„Maßnahmen (gefordert werden), die eine datensparsame Gestaltung der in Telekommunikationsnetzen verwendeten Geräte, Programme und Übertragungswege vorsehen... Um die Gebote der Datensparsamkeit und der Datenvermeidung zu erfüllen, sollte die anonyme und pseudonyme Nutzung der neuen Dienste gefördert werden.“* (Drucksache 13/11004).

Auf den datenschutzrechtlichen Grundsatz des **Verbots einer Vorratsdatenspeicherung** wurde im übrigen auch von der Bundesregierung verwiesen, als ein Verlangen des Bundesrates nach der Vorgabe von Mindestspeicherfristen von Kundendaten gefordert wurde: *„Damit würde den in § 89 Abs. 1 Satz 2 normierten Grundsätzen der Verhältnismäßigkeit, Erforderlichkeit und Zweckbindung ...... widersprochen. Die Verarbeitung von Telekommunikationsdaten ist regelmäßig auf den betrieblich erforderlichen Zweck der Abwicklung der jeweiligen vertraglich vereinbarten Telekommunikationsdienstleistung beschränkt. Das Anliegen des Bundesrates würde vom Ergebnis her auf eine mangels aktuellen Bedarf unzulässige Vorratsspeicherung von Daten hinauslaufen.“* (Drucksache 13/4438, S. 39).

Aus Sicht des Datenschutzes bieten die Prepaid-Verfahren die besten Voraussetzungen für die Realisierung eines sicheren elektronischen Zahlungsverfahrens,

das die gleiche **Anonymität des Bezahlens** erlaubt wie das Bezahlen mit Bargeld. Ich sehe es daher als dringend geboten an, die Diskussion zur Zulässigkeit der Erhebung von Kundendaten im Zusammenhang mit der Nutzung von Prepaid-Cards neu zu beleben und hoffe, daß künftig von einer derartigen Vorratsspeicherung von Daten abgesehen wird.

Die schon erwähnte Telefonkarte der DTAG, von der bereits viele Millionen verkauft wurden, weist den richtigen Weg:

Die letzte habe ich in meinem Zeitschriftenladen gekauft, ohne daß die Inhaberin einen Personalausweis verlangt hätte.

10.2.3 Kreditkartentelefone haben ein langes Gedächtnis

Artikel 10 des Grundgesetzes garantiert die Unverletzlichkeit des Fernmeldegeheimnisses. Gemäß § 85 TKG unterliegt dem besonderen Schutz des Fernmeldegeheimnisses nicht nur der **Inhalt der Telekommunikation**, wie z. B. ein Telefonat, eine Fax-Sendung oder eine e-mail. Auch die **näheren Umstände der Telekommunikation**, also wer wann von wo wie lange und mit wem telefoniert hat – die sog. Verbindungsdaten – werden vom Fernmeldegeheimnis geschützt.

Zur Gewährleistung dieses besonderen Schutzes schreibt die TDSV u. a. vor, wie lange und in welcher Form die Verbindungsdaten gespeichert werden dürfen. Die Verordnung bestimmt weiterhin, daß die Zielrufnummer in der Abrechnung mit dem Kunden nur dann erscheinen darf, wenn der Kunde dies ausdrücklich wünscht (sog. Einzelverbindungsnachweis), und auch nur in der von ihm gewünschten Form (gekürzt oder vollständig). Inzwischen dürfte es allgemein bekannt sein, daß der Kunde von seinem TK-Unternehmen (Festnetz- oder Mobilfunk) verschiedene Arten von Einzelverbindungsnachweisen beantragen kann.

Eine besondere Art von Einzelverbindungsnachweisen kann allerdings bei der Nutzung von Kreditkartentelefonen entstehen, wie sie z. B. an Flughäfen oder Autobahnraststätten zu finden sind. Um von ihnen aus in alle Welt telefonieren zu können, benötigt man kein Geld, sondern lediglich eine Kreditkarte einer der weltweit vertretenen Kreditkartenanbieter (z. B. American Express, Visa usw.). Im vergangenen Jahr bin ich darauf aufmerksam geworden, daß auf den Kreditkartenabrechnungen von Kunden, die Kreditkartentelefone einer bestimmten Firma benutzt hatten, neben dem Betrag, dem Datum, der Uhrzeit des Beginns und des Endes des Telefonats sowie dem Standort des benutzten Telefones auch die vollständige Zielrufnummer des angerufenen Anschlusses auf der Kreditkartenrechnung erschien.

Nachdem ich das betroffene Unternehmen darauf hingewiesen hatte, daß dies ohne vorherige Einwilligung des Kunden unzulässig ist, wurde mir zugesagt, die Abrechnung mit dem Kreditkartenunternehmen künftig ohne die Angabe von Verbindungsdaten vorzunehmen.

Wie sich bei einer Kontrolle herausstellte, hat das betreffende TK-Unternehmen den Datensatz an die Kreditkartenunternehmen tatsächlich erheblich reduziert. In der Abrechnung erscheinen nur noch eine Standortnummer, die Art der in Anspruch genommenen TK-Leistung (z. B. Fax, Telefon) sowie die verkürzte Zielrufnummer. Letztere wurde von dem Unternehmen auf der Kreditkartenrechnung angegeben, um unnötige Reklamationen (z. B. weil sich der Kunde nicht an das Telefonat erinnern kann) zu vermeiden.

Auch dieses Verfahren verstößt noch gegen den Datenschutz:

Zum einen handelt es sich auch bei der verkürzten Zielrufnummer um ein Verbindungsdatum, das nur aufgrund einer telekommunikationsspezifischen Rechtsvorschrift an Stellen außerhalb des Telekommunikationsunternehmens übermittelt werden darf. Eine Vorschrift für die Übermittlung solcher Verbindungsdaten an ein Kreditkartenunternehmen existiert jedoch nicht; erforderlich wäre also die Einwilligung des Kunden. Zum anderen dürfen auch verkürzte Zielrufnummern nur auf ausdrücklichen Wunsch des Kunden in einem Einzelverbindungsnachweis aufgenommen werden.

Um den Erfordernissen des Telekommunikationsdatenschutzes gerecht zu werden, soll der Kunde daher künftig im Display der Kartentelefone darauf hingewiesen werden, daß Verbindungsdaten an das Kreditkartenunternehmen übermittelt und die verkürzten Zielrufnummern in der Kreditkartenabrechnung ausgedruckt werden. Benutzt er das Telefon in Kenntnis dieses Übermittlungsvorganges, darf von seiner Zustimmung ausgegangen werden.

Außerdem mußte ich feststellen, daß die Verbindungsdaten weit über den zulässigen Zeitraum von 80 Tagen nach Rechnungsversand hinaus bei dem betreffenden TK-Unternehmen gespeichert blieben. Dies wurde für erforderlich gehalten, da die Kunden einiger ausländischer Kreditkartenunternehmen bis zu einem Jahr nach Erhalt der Kreditkartenabrechnung hiergegen Einwände erheben können. Auf mein Betreiben hin wurden die Speicherfristen bei dem TK-Unternehmen inzwischen an die telekommunikationsspezifischen deutschen Datenschutzvorschriften angepaßt.

10.2.4 Einzelverbindungsnachweis für das Handy an den Arbeitgeber

Die einen verwünschen das Handy – nicht nur während eines Konzerts –, andere können sich nicht mehr vorstellen, ohne seine Hilfe ihren beruflichen Verpflichtungen überhaupt noch nachkommen zu können. Zu letzteren zählen die im Außendienst Beschäftigten, denen es oft von ihrem Arbeitgeber zur Verfügung gestellt wird. Bei allem Komfort und unbestrittenen Nutzen verursacht das Firmenhandy aber auch immer wieder Probleme. Dies liegt nicht nur an der ständigen Erreichbarkeit seiner Beschäftigten, die den Chef meist freut, aber die Betroffenen wohl nicht immer. Zu Verärgerungen und Auseinandersetzungen führt immer wieder die Möglichkeit zu erfahren, welcher Mitarbeiter wann wo wie lange mit wem telefoniert hat. Dabei ist zu betonen, daß diese „näheren Umstände der Telekommunikation“ vom Fernmeldegeheimnis – einem Grundrecht – geschützt sind.

Die Nutzer solcher vom Arbeitgeber zur Verfügung gestellten Handies sehen die hierbei entstehenden Verbindungsdaten als besonders schützenswert an. Das belegen viele Anfragen und Beschwerden, in denen ich gebeten worden bin, der Frage nachzugehen, ob es zulässig ist, wenn der Arbeitgeber zu den seinen Mitarbeitern zur Verfügung gestellten Mobilfunkanschlüssen – Handies, aber auch Autotelefone – vom TK-Unternehmen sog. Einzelverbindungsnachweise (EVN) erhält.

Hierzu ist grundsätzlich folgendes anzumerken:

Für den Telefonkunden – auch für den Chef – ist es sicherlich von großem Nutzen, wenn er seine Rechnung nicht nur in der bekannten pauschalierten Form bekommt, sondern wenn die Gespräche in einem EVN detailliert aufgelistet sind. Er kann besser die Korrektheit der Rechnung überprüfen und ggf. auch feststellen, wer teure Gespräche verursacht. Aus meiner Sicht bestehen hiergegen grundsätzlich keine Bedenken. Wichtig ist es jedoch, daß durch die Herausgabe des EVN keine Persönlichkeitsrechte der betroffenen Anrufer und Angerufenen verletzt werden. Daher habe ich mich stets mit Nachdruck dafür eingesetzt, daß ein Kunde zwar – auf Wunsch – einen EVN erhält, er aber auch die Persönlichkeitsrechte der Mitbenutzer seines Telefons achtet.

Für Arbeitgeber, die ihren Mitarbeitern Handies zur Verfügung stellen, sieht § 6 Abs. 7 TDSV ausdrücklich vor, daß die TK-Unternehmen auf Antrag einen EVN mit vollständigen Zielrufnummern nur erstellen dürfen, wenn der Arbeitgeber gegenüber dem TK-Unternehmen zuvor schriftlich erklärt hat, daß

– die Mitarbeiter informiert worden sind und künftige Mitarbeiter unverzüglich informiert werden und
– der Betriebsrat oder die Personalvertretung entsprechend den gesetzlichen Vorschriften beteiligt wurden oder eine solche Beteiligung nicht erforderlich ist.

Eine Zustimmung der Arbeitnehmer ist – unabhängig davon, ob nur geschäftliche oder auch private Nutzung des Anschlusses zugelassen ist – nicht erforderlich.

Aufgrund der Eingaben, die mich hierzu erreicht haben, habe ich einzelne TK-Unternehmen und -diensteanbieter nochmals auf die geltende Rechtslage – insbesondere die genannten Erklärungspflichten des Arbeitgebers – nachdrücklich hingewiesen.

10.2.5 Einzelverbindungsnachweis, immer wenn der Kunde es will

Der Kunde hat mehrere Möglichkeiten zu bestimmen, wie seine Telefonrechung aussehen soll. So kann er unter anderem einen Einzelverbindungsnachweis (EVN) fordern, aus dem die Verbindungsdaten der einzelnen von ihm geführten Telefonate ersichtlich sind. Die Voraussetzungen für einen EVN sind in § 6 Abs. 4 und 7 TDSV geregelt. Seit Inkrafttreten der Telekommunikations-Kundenschutzverordnung im Januar 1998 hat jeder Kunde eines TK-Unternehmens außerdem das Recht, diesen EVN kostenlos zu erhalten. Bis zu diesem Zeitpunkt wurde von den TK-Unternehmen vom Kunden ein Entgelt für diesen Service gefordert.

Der Kunde kann den EVN entweder mit vollständigen oder aber um drei Stellen gekürzten Zielrufnummern erhalten. Ein großes TK-Unternehmen hat dies grundsätzlich auf die Fälle beschränkt, in denen der Kunde sich mit einer Speicherung der Verbindungsdaten für 80 Tage einverstanden erklärt. Dieses Unternehmen habe ich darauf hingewiesen, daß ein EVN nach geltenden Rechtslage auch dann erteilt werden muß, wenn der Kunde sich für die Möglichkeit der vollständigen Löschung seiner Verbindungsdaten spätestens mit Versendung der Rechnung entschieden hat. Dieses Recht ergibt sich aus § 6 Abs. 4 der TDSV. Auch aus Eingaben konnte ich ersehen, daß es sich hierbei nicht nur um eine theoretische rechtliche Variante handelt, sondern daß viele Bürger die Möglichkeit eingeräumt haben wollen, für sich ihr Telefonverhalten zu überprüfen. Dieser Wunsch schließt dann aber nicht ein, daß ihre Verbindungsdaten noch 80 Tage zu speichern sind. Von Seiten des Unternehmens wurde diese Rechtsauffassung zunächst nicht geteilt. Erst nach langer Korrespondenz hat man zugestanden, daß die Vorgaben der TDSV so zu verstehen sind und dem Kunden auch diese Variante angeboten werden muß.

Ende 1998 wurde mir mitgeteilt, daß man zur Zeit technisch noch nicht in der Lage sei, diese Forderung umzusetzen. Es wurde mir aber zugesagt, daß meine Forderung möglichst umgehend für das TK-System des betroffenen Unternehmens realisiert würde.

10.2.6 Eine Rechnung für alle

Im Bereich der Ortsgespräche bleiben viele (Festnetz-) Telefonkunden auch nach der Liberalisierung des Telekommunikationsmarktes ihrer Telefongesellschaft treu. Dies ist im allgemeinen die DTAG, die ihren Kunden als sog. Anschlußnetzbetreiber den Zugang zum öffentlichen Telefonnetz eröffnet. Wegen der von sog. Verbindungsnetzbetreibern angebotenen günstigen Tarife wird aber gerade im Fernbereich gleichzeitig auch über andere TK-Anbieter telefoniert. Will ein DTAG-Kunde mit Hilfe eines solchen Verbindungsnetzbetreibers billiger telefonieren, muß er dessen, von der RegTP vergebene Vorwahlnummer 010xy vor jeder Zielrufnummer wählen, bei einem Telefonat nach München also z. B. den Anschluß 010xy 089 1234567. Dieses Verfahren wird als „call-by-call“ bezeichnet. Ausschließliche Vertragsbeziehungen zur DTAG werden daher heutzutage immer seltener. Um ihr Telefonierverhalten und somit auch die Gesamtkosten „auf einen Blick“ nachvollziehen zu können, möchten viele Kunden nur **eine** Rechnung, die die Forderungen aller in Anspruch genommener TK-Anbieter aufführt.

Diese Möglichkeit hat die Bundesregierung im Sinne der Verbraucher mit § 15 Telekommunikations-Kundenschutzverordnung (TKV) geschaffen. Danach ist dem Kunden von seinem Anschlußnetzbetreiber grundsätzlich eine Rechnung zu erstellen, die auch die Entgelte für die in Anspruch genommenen Verbindungsnetzbetreiber ausweist. Diese verbraucherfreundliche Vorschrift für eine TK-Gesamtrechnung bringt aber datenschutzrechtliche Probleme mit sich.

So verlangt § 6 Abs. 3 TDSV, daß die für die Entgeltberechnung benötigten Verbindungsdaten grundsätzlich 80 Tage nach Versand der Rechnung zu löschen sind. Die Verbindungsnetzbetreiber, die ihre Entgeltdaten für die Erstellung der TK-Gesamtrechnung und zum Forderungseinzug an die DTAG übermitteln, kennen mangels entsprechender Unterrichtung durch die DTAG den Zeitpunkt des Rechnungsversandes aber nicht. Da weder TKV noch TDSV entsprechende Informationspflichten vorsehen, ist ihnen eine korrekte Beachtung der Löschungsfrist von 80 Tagen nicht möglich.

Problematisch ist dies insbesondere beim Telefonieren „call-by-call“. Hier wird zwischen dem Kunden und seinem Verbindungsnetzbetreiber zumeist kein schriftlicher Vertrag geschlossen. Vielmehr besteht zwischen ihnen häufig ein konkludentes, d. h. stillschweigend eingegangenes Vertragsverhältnis, das allein durch die Eingabe einer bestimmten Vorwahlnummer beim Wählvorgang begründet wird (s. o.). Abreden über die konkrete Ausgestaltung des Vertrages werden dabei naturgemäß nur ansatzweise getroffen. Dies gilt auch für die Wahl der Rechnungsform, nämlich pauschalierte Rechnung oder Einzelverbindungsnachweis. In diesen Fällen wird der DTAG nicht bekannt, welche Rechnungsart sich der Kunde von seinem Verbindungsnetzbetreiber wünscht. Dem Kunden muß es aber zugestanden werden, die Vertragsverhältnisse und damit auch die gewählte Rechnungsart je nach TK-Anbieter unterschiedlich gestalten zu können. Dies kann im Einzelfall zur Folge haben, daß er bei der Wahl der Rechnungsform zwischen seinem Anschlußnetzbetreiber und seinem Verbindungsnetzbetreiber differenziert. Derzeit weist die DTAG die ihr übermittelten Entgeltdaten nur dann auf ihren Rechnungen aus, wenn sich ihre Kunden für den Einzelverbindungsnachweis entschieden haben (s. o. Nr. 10.2.5).

Diese datenschutzrechtlichen Probleme, die sich als Folge nicht aufeinander abgestimmter Rechtsvorschriften ergeben, habe ich dem für den Bereich der Telekommunikation zuständigen BMWi vorgetragen. Dort ist man sich der Problematik bewußt. Ich hoffe, daß es im Rahmen der Novellierung der TDSV zu einer entsprechenden, die Belange des Datenschutzes angemessen berücksichtigenden Harmonisierung kommen wird (s. o. Nr. 10.1.3).

10.2.7 Die „Fangschaltung“: Altes Thema, neue Fragen

Nicht immer freuen wir uns über einen Telefonanruf. Ärgerlich sind schon die – unzulässigen! – Anrufe z. B. dubioser Anlageberatungsfirmen, die am Telefon unglaubliche Renditen versprechen. Wirklich schlimm aber sind Telefonate, in denen die Angerufenen – es sind hierbei überwiegend Frauen betroffen – obszön belästigt oder gar bedroht werden. Solange noch wenige Angerufene die Rufnummer des Anrufers am Display ihres Telefones erkennen können, bleibt die „Fangschaltung“ das einzige Mittel, um den – zumeist anonymen – Anrufer ermitteln und belangen zu können.

In einem solchen Fall richtet das TK-Unternehmen dem Kunden eine „Fangschaltung“ auf Antrag ein. Bekommt der Telefonkunde dann einen belästigenden oder bedrohenden Anruf, „markiert“ er ihn z. B. im Telefon-Festnetz durch Tastendruck an seinem Telefon, woraufhin ihm das TK-Unternehmen Zeitpunkt und Rufnummer des Anrufes sowie den Namen und die Anschrift des Inhabers des Telefons mitteilt, von dem der Anruf ausging.

Im Berichtszeitraum ergaben sich im Zusammenhang mit der „Fangschaltung“ einige Probleme, die in den folgenden Berichten dargestellt werden.

10.2.7.1 Buchbinder Wanninger und die Telekommunikation – oder: Die netzübergreifende „Fangschaltung“

Die rechtliche Grundlage für die „Fangschaltung“ ergibt sich aus § 8 Abs. 1 Satz 1 TDSV. Danach ist einem Kunden, der in einem zu dokumentierenden Verfahren schlüssig vorträgt, daß bei seinem Anschluß bedrohende oder belästigende Anrufe ankommen, von seinem TK-Unternehmen auf schriftlichen Antrag – auch netzübergreifend – Auskunft über die Anschlüsse zu erteilen, von denen die Anrufe ausgegangen sind. Dabei dürfen die Rufnummern, Namen und Anschriften der Inhaber dieser Anschlüsse sowie Datum und Uhrzeit des Beginns der Verbindungen und der Verbindungsversuche erhoben, gespeichert und dem Antragsteller mitgeteilt werden.

Sowohl die Bezeichnung „Fangschaltung“ als auch die ihr zugrundeliegende, veraltete Technik stammt aus einer Zeit, als es nur ein TK-Unternehmen gab, nämlich „die Post“. Heute gibt es aber eine Vielzahl solcher Unternehmen und zwar sowohl im Telefon-Festnetz als auch in den Mobiltelefonnetzen. Und seit es Handies gibt, werden auch sie für belästigende und bedrohende Anrufe benutzt.

Die Praxis hat gezeigt, daß in den Fällen, in denen vom TK-Unternehmen des Antragstellers im Rahmen einer „Fangschaltung“ Anrufe aus anderen als dem eigenen Netz ermittelt werden, dem Antragsteller lediglich die „gefangene“ Rufnummer sowie der betreffende Netzbetreiber mitgeteilt wird. („Der Anruf kam von der Rufnummer 471112 aus dem Mobilfunknetz der Fa. XY.“) Es bleibt dann dem Antragsteller überlassen, den Namen und die Anschrift des „Gefangenen“ selbst beim jeweiligen Netzbetreiber zu erfragen.

Dieses Verfahren ist in hohem Maße kundenunfreundlich und auch datenschutzrechtlich mangelhaft.

Nach der genannten Rechtsvorschrift hat das Unternehmen die Auskunft *„auch netzübergreifend“* zu erteilen. Nach Satz 2 der Vorschrift umfassen die Auskünfte dabei neben dem Zeitpunkt auch *„Rufnummern, Namen und Anschriften der Inhaber dieser Anschlüsse.“* Daraus folgt die Verpflichtung der Unternehmen, auch in Fällen einer netzübergreifenden „Fangschaltung“ dem Antragsteller neben der „gefangenen“ Anschlußnummer auch Namen und Anschrift des Inhabers zu nennen und hierfür die erforderlichen Auskünfte beim betreffenden Netzbetreiber einzuholen.

Zu meinem Bedauern wird diese datenschutzrechtliche – und kundenorientierte – Sichtweise von der Regulierungsbehörde für Telekommunikation und Post nicht

geteilt. Sie ist der Auffassung, daß ein Anspruch des Antragstellers gegen „sein“ TK-Unternehmen zur Ermittlung der Daten bei den anderen TK-Unternehmen nicht bestehe, zumal ein entsprechender Auskunftsanspruch der Unternehmen **untereinander** nicht normiert sei. Im Gegensatz hierzu bestehe aber ein Auskunftsanspruch des Antragstellers auch gegenüber dem Unternehmen des Anrufers.

Diese Rechtsauffassung der Reg TP teile ich nicht:

Es kann nicht im Interesse des Antragstellers sein, wenn er in einer Situation, in der er bedroht und belästigt wird, verschiedene TK-Unternehmen anschreiben muß, um den Namen und die Anschrift derjenigen zu erfragen, zu denen die festgestellte Rufnummer gehört. Wie langwierig und schwierig dabei eine Auskunft zu erlangen ist, muß auch ich immer wieder bei der Verfolgung von Beschwerden erfahren: „Das ist aber nicht unser eigener Kunde, sondern der unseres Subunternehmers; da müssen Sie schon den fragen!“ lautet da nicht selten die Auskunft. Wieviel mehr droht da dem „normalen“ Anfrager die Frustration von Karl Valentins Buchbinder Wanninger, der nach 19 Telefonaten immer noch nichts erfahren hat: „Saubande, dreckade!“

Das derzeit von den TK-Unternehmen praktizierte Verfahren muß dahin geändert werden, daß der Antragsteller einer „Fangschaltung“ von seinem TK-Unternehmen die Verursacher **aller** bedrohender oder belästigender Anrufe erfährt – sowohl aus dem eigenen Netz, als auch aus den fremden Netzen.

Ich werde mich im Rahmen der anstehenden Neufassung der TDSV mit Nachdruck dafür einsetzen, daß dies eindeutig in meinem Sinne geregelt wird.

10.2.7.2 Rückwirkende „Fangschaltung“

Aufgrund der Anfrage eines TK-Unternehmens war der Frage nachzugehen, ob die Ermittlung der Anschlüsse, von denen belästigende Anrufe ausgingen, nach § 8 TDSV auch für die Vergangenheit durchführbar ist. Technisch ist dies unter gewissen Voraussetzungen möglich:

Kann der Kunde den Zeitpunkt eines solchen Anrufes genau angeben („Vorgestern, um 23.41 Uhr“) und ist ein solcher Verbindungsdatensatz noch gespeichert, könnte das Unternehmen diesen – und damit auch den Verursacher des Anrufes – ermitteln.

Nach § 8 Abs. 1 TDSV hat ein TK-Unternehmen seinem Kunden unter den dort im einzelnen aufgeführten Voraussetzungen Auskünfte über die Anschlüsse zu erteilen, *„von denen bedrohende oder belästigende Anrufe ausgegangen sind.“* Aufgrund der vom Verordnungsgeber gewählten Vergangenheitsform kann die Auskunftspflicht der TK-Unternehmen und TK-Diensteanbieter nicht auf künftige Anrufe beschränkt werden. Vielmehr muß schon nach dem Wortlaut der Vorschrift davon ausgegangen werden, daß grundsätzlich auch vergangene, d. h. vor der Beantragung einer „Fangschaltung“ erfolgte Anrufe, vom Regelungsumfang der Vorschrift erfaßt werden sollen.

Auch Sinn und Zweck der Bestimmung zufolge ist eine Verpflichtung zur Durchführung von „Fangschaltungen“ für die Vergangenheit anzunehmen. Die „Fangschaltung“ stellt zwar regelmäßig einen Eingriff in das Fernmeldegeheimnis des Anrufers dar. Das Bundesverfassungsgericht hat in seiner sog. Fangschaltungsentscheidung (BVerfGE 85, 386ff.) jedoch festgestellt, daß dieser Eingriff in bestimmten Fällen gerechtfertigt ist. Andernfalls würde die Verweigerung der Einrichtung einer „Fangschaltung“ grundrechtlich geschützte Belange anderer Fernsprechteilnehmer beeinträchtigen, die Opfer bedrohender oder belästigender Anrufe werden. Solche Anrufe können das allgemeine Persönlichkeitsrecht aus Artikel 2 Abs. 1 i.V.m. Artikel 1 Abs. 1 GG und das Recht auf körperliche Unversehrtheit aus Artikel 2 Abs. 2 GG empfindlich berühren. Die Betroffenen sind derartigen Angriffen schutzlos ausgesetzt. Die Einrichtung einer „Fangschaltung“ bildet hier insofern ein besonders wirksames, oft sogar das einzige Mittel der Gegenwehr. Der Anrufer muß in diesen Fällen einen Eingriff in sein Fernmeldegeheimnis hinnehmen.

Im Rahmen der anstehenden Neufassung der TDSV werde ich mich dafür einsetzen, daß zur Frage der rückwirkenden Feststellung ankommender Verbindungen eine klarstellende Formulierung in die Verordnung aufgenommen wird.

10.2.7.3 Mißbrauchte Fangschaltung: Frauenhäuser beklagten sich

Frauenhäuser und ähnliche Einrichtungen sind oft der letzte Zufluchtsort für Frauen und ihre Kinder, die sich in ausweglos erscheinenden familiären Situationen befinden. Hier finden sie eine zeitweilige, geschützte Unterkunft sowie Rat und Hilfe. Im Interesse der betreuten Frauen müssen diese Einrichtungen höchsten Wert darauf legen, geschützt zu bleiben, d. h. unter anderem auch, daß ihre Anschrift nicht denjenigen bekannt wird, vor denen ihre Schutzbefohlenen geflohen sind.

Viele dieser Einrichtungen empfehlen allerdings den bei ihnen Schutzsuchenden, den Kontakt zu ihren Familien und anderen Angehörigen nicht abzubrechen, ihn wenigstens telefonisch aufrechtzuerhalten und stellen dafür ihren Telefonanschluß zur Verfügung. Eine dieser Einrichtungen informierte mich darüber, daß es in zwei verschiedenen Fällen den Angehörigen junger Frauen, die den Schutz der Einrichtung gesucht hatten, gelungen sei, die Adresse der Einrichtung und damit den Aufenthaltsort der Frauen „mit Hilfe der Telefonfirma“ zu ermitteln.

Die Angehörigen der beiden Frauen hatten zu diesem Zweck bei dem TK-Unternehmen, an dessen Netz ihr Telefon angeschlossen war, eine sog. Fangschaltung nach § 8 TDSV beantragt. Diese war ihnen nach der genannten Vorschrift nur zugestanden worden, weil sie behauptet hatten, „bedrohende und belästigende Anrufe" erhalten zu haben. Das TK-Unternehmen ist in solchen Fällen verpflichtet, eine Fangschaltung einzurichten; ob wirklich solche Anrufe eingegangen sind, kann und braucht es nicht überprüfen. Riefen nun die in der Einrichtung lebenden Frauen ihre Familien an, wurden die Anrufe von der jeweiligen Telefonfirma registriert und

den Antragstellern anschließend mitgeteilt, von welchem Anschluß sie ausgingen – hier also Name, Adresse und Telefonnummer des Frauenhauses. Nachdem das Frauenhaus so mißbräuchlich „enttarnt" worden war, wurde in einem Fall sogar noch versucht, eine Frau gewaltsam von dort zu entführen, was nur durch das beherzte Eingreifen von Bürgern verhindert werden konnte.

Aufgrund des Hinweises des Frauenhauses habe ich zunächst einmal erreicht, daß das TK-Unternehmen, bei dem das Frauenhaus Kunde ist, im Zusammenhang mit Fangschaltungen nur noch allgemein Auskunft erteilt, damit das Frauenhaus nicht enttarnt wird. Darüberhinaus habe ich dem TK-Unternehmen empfohlen, grundsätzliche Lösungen zu finden, die einerseits nicht den Zweck des § 8 TDSV (Erkennen der Verursacher von bedrohenden oder belästigenden Anrufen) unterlaufen, andererseits aber den Schutz solcher Einrichtungen vor „Enttarnung“ durch mißbräuchliche Nutzung des vorgeschriebenen Verfahrens sicherstellen.

Das TK-Unternehmen hat mittlerweile sein Verfahren bezüglich der Bekanntgabe der Anschlüsse von Frauenhäusern und ähnlichen Einrichtungen neu gestaltet. Wird bei dem Unternehmen im Rahmen der Auswertung einer Fangschaltung künftig als „gefangene“ Nummer die eines Frauenhauses erkannt, erscheint auf dem Bearbeitungsbildschirm – noch vor der Anzeige der Adresse – ein spezieller Warnhinweis, der nur von besonders berechtigten Mitarbeitern gelöscht werden kann, die dann auch die weitere Bearbeitung übernehmen. Als Adresse des Frauenhauses wird dem Antragsteller eine – mit dem Frauenhaus vereinbarte – Angabe gemacht, die bis auf die Postleitzahl keine Rückschlüsse auf den konkreten Standort zuläßt. Dabei wird die Telefonnummer nicht mitgeteilt.

Ich meine, daß damit eine Lösung gefunden wurde, die sowohl dem Willen des Gesetzgebers als auch dem berechtigten Schutzanspruch dieser wichtigen Einrichtungen und ihrer Bewohnerinnen Rechnung trägt.

Es liegt jedoch an jeder einzelnen Einrichtung selbst, die Initiative zu ergreifen, ob das geschilderte Verfahren auf sie angewandt wird. Sie muß sich dazu mit ihrem TK-Unternehmen in Verbindung setzen und die erforderlichen Absprachen treffen.

Dem von der Beschwerde betroffenen TK-Unternehmen danke ich für sein konstruktives Herangehen an die Lösung dieses Problems. Ich gehe davon aus, daß es vergleichbare Fälle genauso verantwortungsvoll prüft, auch wenn es hierzu keine gesetzliche Verpflichtung gibt.

10.2.8 Rufnummernübermittlung: Ein vielgestaltiges Thema

10.2.8.1 Der Kunde entscheidet, ob seine Rufnummer übermittelt wird

Wer kennt nicht die sich alltäglich oft wiederholende Situation – das Telefon klingelt und man fragt sich: „Wer mag da wohl jetzt anrufen?“ Soll man das Gespräch annehmen oder das Telefon, weil man vielleicht gerade vermeintlich Wichtigeres zu tun hat, einfach klingeln lassen – was auch nervend sein kann.

In solchen Fällen kann das sowohl im Festnetz als auch in den Funktelefonnetzen angebotene Leistungsmerkmal der sog. Rufnummernübermittlung – auch CLIP (calling line identification presentation) genannt – von besonderem Nutzen sein. Hierbei wird die Rufnummer des Anrufers zum Telefonanschluß des Angerufenen übertragen und kann an dessen Telefon oder Handy angezeigt werden. Den Angerufenen versetzt das in die Lage zu entscheiden, ob er den Anruf annimmt oder es weiter klingeln läßt.

Im ISDN-Netz war die Rufnummernübermittlung von Anfang an realisiert. Insbesondere in öffentlichen Dienststellen und Unternehmen, die über eine moderne TK-Anlage verfügen, wurde die Rufnummernübermittlung bereits zu einem frühen Zeitpunkt eingeführt und bekannt. Im „normalen“ Festnetz wird das Leistungsmerkmal der Rufnummernübermittlung, das etwa Ende 1997 bundesweit technisch realisiert wurde, bislang noch selten genutzt.

Auch wenn die Rufnummernübermittlung einerseits durchweg sinnvoll und nützlich sein mag, so darf andererseits jedoch nicht übersehen werden, daß es Situationen gibt, in denen der Anrufer nicht unbedingt eine Rufnummernübermittlung wünscht, d. h. vom Angerufenen weder erkannt noch gespeichert werden möchte. Ruft man beispielsweise bei verschiedenen Banken an, um sich nach den aktuellen Darlehenszinsen zu erkundigen, kann nicht ausgeschlossen werden, daß sich der angerufene Bankangestellte die ihm übermittelte Rufnummer notiert, um den Anrufer zu einem späteren Zeitpunkt z. B. mit anderen Dienstleistungen der Bank zu bewerben, was dieser aber nicht beabsichtigt hatte.

Die Rufnummernübermittlung ist ein Thema des Datenschutzes, seit es sie gibt. Erst die TDSV hat hierzu Vorschriften erlassen.

Aufgrund der Regelungen in § 9 TDSV hat der Diensteanbieter, der Anschlüsse anbietet, die die Rufnummer des Anrufenden an den angerufenen Anschluß übermitteln, dem anrufenden Kunden hinsichtlich der Anzeige seiner Rufnummer kostenfrei die Wahl zwischen drei Varianten einzuräumen, nämlich

1. den dauernden Ausschluß der Anzeige,
2. den Ausschluß der Anzeige nur bei bestimmten Anrufen oder
3. der Anzeige der Rufnummer bei jedem Anruf.

In der jüngeren Zeit hat mich die Rufnummernübermittlung immer wieder beschäftigt. So war u. a. zu prüfen, ob die DTAG – als Vertragspartner von über 40 Millionen Telefonkunden – bei der Gestaltung der von den Kunden auszufüllenden Auftragsvordrucke entsprechend den rechtlichen Vorgaben der TDSV verfährt.

Bei allen Neukunden der DTAG ist das Leistungsmerkmal „Rufnummernanzeige“ seit Januar 1998 Gegenstand des mit dem Kunden abgeschlossenen Vertrages. Dem-

zufolge sieht auch der Auftragsvordruck für einen Telefonanschluß ein entsprechendes Wahlrecht für den Kunden vor. Danach kann er sich für die ständige Übermittlung der Rufnummer oder für die Möglichkeit entscheiden, die Rufnummernanzeige durch Tastendruck am Telefon zu unterdrücken, wenn man seine Telefonnummer nicht weitergeben will. Die dritte Variante – die ständige Unterdrückung der Rufnummernanzeige – ist vom Kunden gesondert zu beauftragen. Die Auftragsgestaltung entspricht somit den rechtlichen Anforderungen.

Bei Altkunden wird die Rufnummernübermittlung nur dann – und zwar kostenfrei – eingerichtet, wenn Kunden dies ausdrücklich wünschen.

Auf Nachfrage hat mir das Unternehmen nochmals ausdrücklich bestätigt, daß die Weitergabe der Rufnummer zum angerufenen Anschluß nur dann realisiert wird, wenn

– der Kunde des **anrufenden Anschlusses** die Weitergabe der Rufnummer durch seinen Auftrag bzw. seine Einwilligung veranlaßt und auch
– der Kunde des **angerufenen Anschlusses** die Anzeige der übermittelten Rufnummern beauftragt hat.

Nur wenn die zuvor genannten Bedingungen erfüllt sind, kann ein geeignetes Telefon oder auch ein anderes Endgerät die Rufnummer des Anrufers anzeigen.

Nicht zu vergessen sind in diesem Zusammenhang die Telefonzellen. Nach Auskunft der DTAG sind diese so geschaltet, daß eine Rufnummernübermittlung beim Angerufenen nicht erfolgt.

Bei an das ISDN-Netz der DTAG angeschlossenen **TK-Anlagen** – früher zumeist Nebenstellenanlagen genannt – sind in der Regel die technischen Voraussetzungen gegeben, daß bei abgehenden Gesprächen die Rufnummer des Anrufers beim Angerufenen angezeigt wird. Die Problematik der Rufnummernanzeige ist daher auch im Zusammenhang mit dem Telefonverkehr von Wirtschaftsunternehmen und Behörden von Interesse; bei letzteren beschränkt sich meine Zuständigkeit auf solche des Bundes. Hier ist das im Zusammenhang mit der privaten Nutzung einer solchen TK-Anlage bestehende Recht auf informationelle Selbstbestimmung der Mitarbeiter im Rahmen einer angemessenen, ordungsgemäßen und wirtschaftlichen Nutzung von TK-Anlagen durch die bei der jeweiligen Dienststelle eingerichtete Personalvertretung wahrzunehmen (§ 75 Abs. 3 Nr. 17 BPersVG). Die vom Gesetzgeber vorgesehene Beteiligung des Personalrates erfolgt in aller Regel durch den Abschluß einer **Dienstvereinbarung** zwischen der Dienststelle und dem Personalrat oder eine nur mit Zustimmung des Personalrates in Kraft zu setzende Dienstanweisung zur Nutzung der TK-Anlage. Ich halte es für geboten, auch das Leistungsmerkmal der Rufnummernanzeige in entsprechende Dienstvereinbarungen/Dienstanweisungen aufzunehmen. Im übrigen sind die Beschäftigten in angemessener Weise über die technischen Möglichkeiten der in der Behörde installierten TK-Anlage (einschließlich des Leistungsmerkmals der Rufnummernanzeige) in Kenntnis zu setzen.

Die gleiche Problematik gilt auch für die private Nutzung der TK-Anlage in einem Betrieb durch die Beschäftigten.

10.2.8.2 Telefonauskunft auch an Rettungsdienste möglich

Im Zusammenhang mit der vorstehend erläuterten Rufnummernübermittlung hatte ich mich im Herbst 1997 erstmals mit einer besonderen Fragestellung auseinanderzusetzen, bei der es im wortwörtlichen Sinne „um Leben oder Tod“ gehen kann.

In der zum damaligen Zeitpunkt neu installierten Rettungsleitstelle in München mit der Notrufnummer 112 wurde aufgrund technischer Neuerungen die Rufnummer des Anrufers an die Rettungsleitstelle übermittelt, was gemäß § 9 Abs. 5 TDSV zulässig ist. In einem bei der Rettungsleitstelle aufgelaufenen Notruf hatte ein Anrufer, der auch in einem mehr als halbstündigen Gespräch nicht bereit war, seine Adresse zu nennen, seinen Selbstmord angekündigt. Die Rettungsleitstelle in München fragte daraufhin das betreffende TK-Unternehmen nach der Adresse dieses Anrufers. Das verweigerte jedoch die Auskunft und verwies auf *„datenschutzrechtliche Bestimmungen“*.

Nach dem „Buchstaben des Gesetzes“ befand sich das TK-Unternehmen dabei im Recht: Die Gestaltung von Auskunftsdiensten im Bereich der Telekommunikation richtet sich nach § 11 Abs. 5 TDSV, wonach *„die Auskunftserteilung über Namen und andere Daten von Kunden, von denen nur die Rufnummer bekannt ist“,* unzulässig ist. Sonderfälle, wie den der Rettungsleitstelle, kennt die TDSV leider nicht. Daher kann die Weigerung, die Adresse eines seiner Kunden über die **„normale Telefonauskunft“** an die Rettungsleitstelle herauszugeben, formalrechtlich nicht kritisiert werden. Sachgerecht ist es jedoch, wenn die Rettungsleitstellen in solchen Notfällen die erforderlichen Auskünfte von einer **besonderen Ansprechstelle** des Unternehmens erhalten können, z. B. derjenigen, die auch den Sicherheitsbehörden die ihnen zustehenden Auskünfte nach § 89 Abs. 6 TKG erteilt (s. o. Nr. 10.1.5.3). Diese könnte dann durch einfache Maßnahmen auch einem Mißbrauch entgegenwirken, z. B. prüfen, ob es sich bei dem Anfragenden wirklich um die Rettungsleitstelle München handelt.

Für die datenschutzrechtliche Beurteilung kommt es daher darauf an, ob die genannte Rettungsleitstelle in München – unabhängig von § 11 TDSV – aufgrund einer gesetzlichen Bestimmung oder durch Rechtsverordnung einen Anspruch gegen das TK-Unternehmen auf Herausgabe von Kundenanschriften geltend machen kann, z. B. zur Abwehr von Gefahren für die öffentliche Sicherheit oder Ordnung i.S.v. § 89 Abs. 6 TKG.

Die von den Rettungsdiensten in Bayern wahrgenommenen Aufgaben sind im Bayerischen Rettungsdienstegesetz geregelt. Dieses ordnet die Tätigkeit der Rettungsdienste nicht nur der Gesundheitsfürsorge zu, sondern stellt sie daneben auch als Aufgabe der allgemeinen Gefahrenabwehr dar. Die Rettungsleitstellen, die alle Einsätze der Rettungsdienste lenken und aufeinander abstimmen, sind dementsprechend ebenfalls als Behörden zur allgemeinen Gefahrenabwehr zu beurteilen.

Aus meiner Sicht bestehen somit in solchen Notfällen keine datenschutzrechtlichen Bedenken gegen die Bekanntgabe der Adresse eines Anrufers durch das TK-Unternehmen. Wegen der Zuweisung zahlreicher, nicht immer ausschließlich der allgemeinen Gefahrenabwehr zurechenbarer Aufgaben an die Rettungsleitstellen ist die grundsätzlich gegebene Auskunftsmöglichkeit nach § 89 Abs. 6 TKG aber stets im jeweiligen Einzelfall zu prüfen, was – anders als die „normale Telefonauskunft“ – die besonderen Ansprechstellen der TK-Unternehmen sehr wohl tun können.

10.2.9 Die Anrufweiterschaltung: Aber nicht heimlich!

Wer kennt nicht die Situation: Man erwartet einen wichtigen Anruf und geht aus Sorge, ihn zu versäumen, nicht aus dem Haus, obwohl der übliche Sportabend stattfindet. In der beruflichen Umgebung – wo heute im allgemeinen eine moderne TK-Anlage (s. o. Nr. 10.1.9) zur Verfügung steht – kann man das Problem durch eine sogenannte Anrufweiterschaltung lösen: Wer immer beispielsweise die Nr. 123 im Büro anruft, erreicht stets die Nr. 456, zu der weitergeleitet wurde.

Auch im Festnetz der DTAG und in den Mobilfunknetzen steht die Möglichkeit der Anrufweiterschaltung jetzt zur Verfügung. Damit erreicht uns der wichtige Anruf auch in der Sporthalle! Nach § 9 Abs. 4 TDSV muß jedoch im Fall der Anrufweiterschaltung vom TK-Unternehmen *„sichergestellt werden, daß diese Tatsache dem Anrufer mitgeteilt wird, soweit dies technisch möglich ist.“* Diese Vorschrift trägt dem Umstand Rechnung, daß die allermeisten Anrufer – jedenfalls jetzt noch – davon ausgehen, durch einen Telefonanruf einen bestimmten anderen in dessen eigener Umgebung zu erreichen, z. B. den Freund in seiner Wohnung, den Hausarzt in der Praxis. Keinesfalls aber möchte ein Petent, wie er mir schrieb, daß sein Hausarzt seinen Anruf etwa in dessen Stammkneipe entgegennimmt.

Die Signalisierung der Anrufweiterschaltung – akustisch oder durch Display-Anzeige – soll also dem Anrufer ermöglichen, sein informationelles Selbstbestimmungsrecht insofern auszuüben, als er entscheidet, ob er den Angerufenen trotz einer Anrufweiterschaltung erreichen will.

Ein großes TK-Unternehmen hat im Berichtszeitraum die bis dahin bestehende automatische Hinweisansage *(„Wir verbinden weiter“)* deaktiviert. Begründet wurde dies mit *„vorhergesehenen technischen Schwierigkeiten“*, die allerdings nur angedeutet wurden. Damit waren nach dortiger Auffassung die Voraussetzungen für die Hinweisansage aus *„technischen Gründen“* nicht mehr gegeben.

In diesem Zusammenhang habe ich dem seinerzeit zuständigen BMPT mitgeteilt, daß – unter bestimmten Voraussetzungen gelegentlich auftretende – „technische Schwierigkeiten“ keinesweg die Diensteanbieter von ihrer Rechtspflicht befreien. Datenschutzrechtlich sei die Deaktivierung der Hinweisansage nur dann vertretbar, wenn die „technischen Gründe“ benannt und nach Beseitigung die Hinweisansage unverzüglich wieder aktiviert würde. Das BMPT teilte mir daraufhin mit, daß es auf das TK-Unternehmen dahingehend einwirken werde, daß die aus § 9 Abs. 4 TDSV resultierenden Anforderungen erfüllt würden, sobald dies technisch möglich sei.

Nachdem das TK-Unternehmen bis Sommer 1998 noch immer keine Lösung der technischen Schwierigkeiten gefunden hatte, habe ich die RegTP um Prüfung der technischen Möglichkeit – und der Probleme – der Realisierung der Hinweisansage der Anrufweiterschaltung gebeten.

Diese hat mir mitgeteilt, daß bei normalen Verbindungen – nämlich zwischen Standard-Telefonen – aus technischer Sicht der problemlose Betrieb gewährleistet wäre, wenn bei der Anrufweiterschaltung die Hinweisansage aktiviert sei. Für bestimmte Anschlüsse könne es jedoch zu erheblichen technischen Problemen kommen. Dies gelte z. B. bei Anrufweiterschaltungen der Notrufnummern von Rettungsdiensten zum Anruf durch Behinderte, Kranke oder Senioren sowie bei Anrufweiterschaltungen der Anschlüsse von Alarmanlagen, Pegelmeldern, Faxgeräten, Modems usw. In diesen Fällen könne es dazu kommen, daß der Betrieb erheblich behindert werde mit der Folge, daß etwa ein Notruf nicht auswertbar sei.

Bei Anschlüssen dieser Art braucht das TK-Unternehmen daher aufgrund der Vorschrift des § 9 Abs. 4 TDSV keine Hinweisansage oder ähnliches vorzusehen.

Für alle anderen als die zuvor genannten Anschlüsse – für die ganz überwiegende Mehrheit der „normalen Telefone“ also – muß die Forderung des § 9 Abs. 4 TDSV aber erfüllt werden. Daher habe ich das TK-Unternehmen aufgefordert, die Hinweisansage oder eine andere, möglicherweise geeignetere Signalisierung unverzüglich (wieder) zu aktivieren. Bei Redaktionsschluß war das allerdings immer noch nicht geschehen. Ich werde es nicht hinnehmen, daß hier wegen technischer Schwierigkeiten ein Rechtsanspruch von Telefonkunden mißachtet wird.

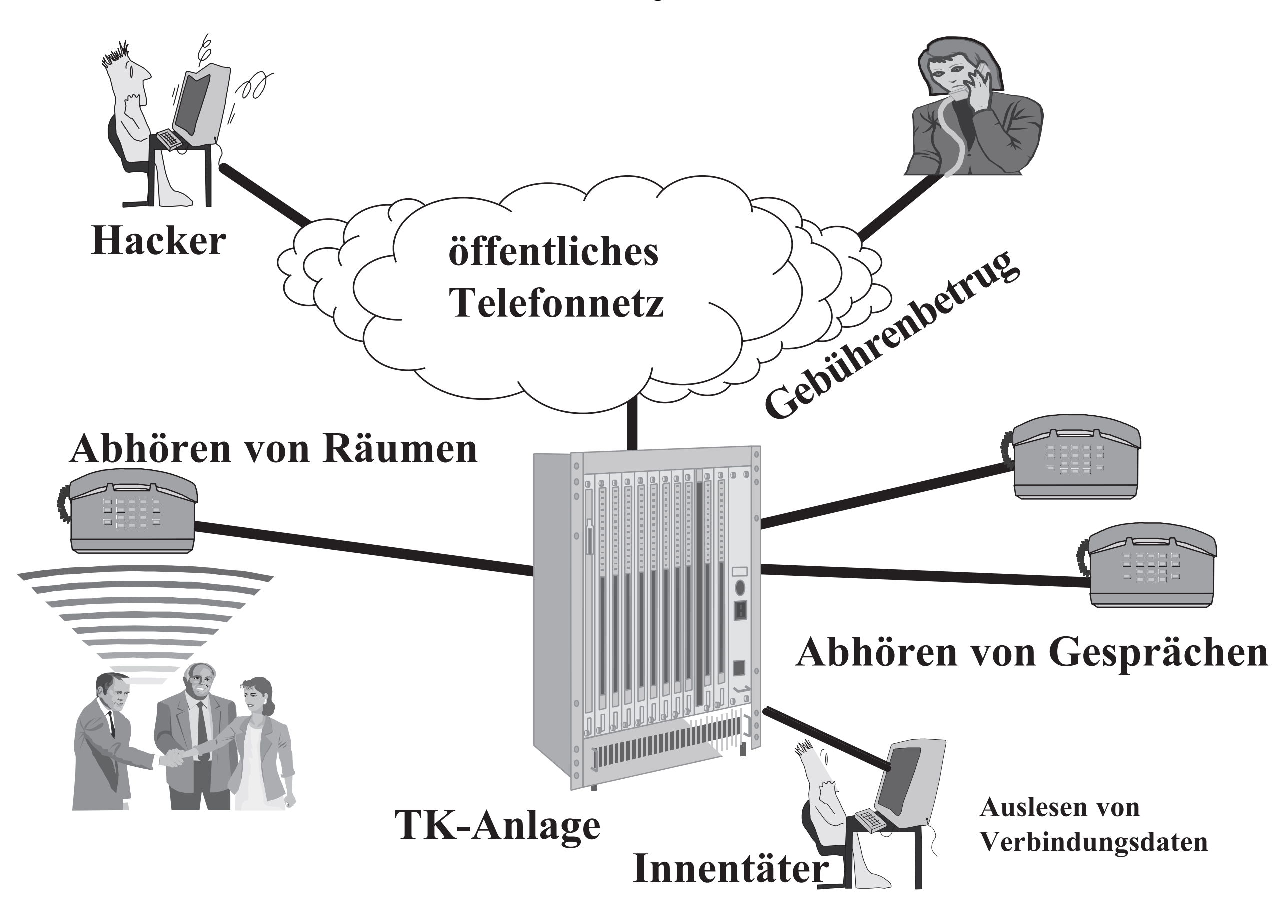
10.2.10 Angriff auf den D-Kanal

Seit einiger Zeit bieten die TK-Netzbetreiber nicht nur „normale“ Telefonanschlüsse an, sondern auch sog. „ISDN-Anschlüsse“. Das Integrated Services Digital Network (ISDN) ist eine Technik innerhalb der Telekommunikation, mit der sich Daten und Sprache ohne Zusatzgeräte (Modem usw.) übertragen lassen. Dabei ist ISDN nicht nur weniger störanfällig als die normale (analoge) Übertragungstechnik, sondern läßt auch eine wesentlich schnellere Datenübertragung zu. Die weite Verbreitung der ISDN-Technik bei den TK-Netzbetreibern hat zur Folge, daß auch die Anbieter von TK-Anlagen (früher auch als „Nebenstellenanlagen“ bezeichnet) ihr Angebot auf diesen Markt ausrichten.

Verbunden mit der Umstellung von der bisherigen Analogtechnik auf die neue Digitaltechnik ist auch eine veränderte Gefährdungslage entstanden. Ich hatte bereits in

Abbildung 9 (zu Nr. 10.2.10)

Gefahren beim Einsatz einer ISDN-TK-Anlage ohne Schutz durch einen D-Kanal-Filter



meinem 15. TB (Nr. 20.2.10) auf die neuen Gefahren hingewiesen. Die Situation hat sich allerdings seit den damaligen Feststellungen nicht entspannt, sondern durch die schnelle Verbreitung der ISDN-Technik und die Veröffentlichung verschiedener Methoden des Angriffs auf TK-Anlagen sogar noch verschärft.

Die meisten Angreifer benutzen dabei eine Schwachstelle der ISDN-Technik, den sog. D-Kanal. Im Gegensatz zur herkömmlichen analogen Technik, bei der lediglich **eine** Verbindung – z. B. ein Telefonat – über eine Leitung möglich ist, lassen sich im ISDN gleichzeitig **zwei Nutzkanäle** (B1- und B2-Kanal) mit einer Übertragungsrate von je 64 kBit/s und zusätzlich noch ein Steuerkanal, dem D-Kanal, mit 16 kBit/s, betreiben. Ermöglicht wird dies durch Zeitfenster, die dem B1-, B2- und D-Kanal abwechselnd zugewiesen werden. Die Übertragung der einzelnen Kanäle erfolgt also gewissermaßen zeitlich versetzt und zwar so schnell, daß der Teilnehmer davon nichts merkt. Die Kanäle B1 und B2 werden dabei ausschließlich für die Übertragung der Nutzinformation verwendet, z. B. der eine für ein Telefonat, der andere – zeitgleich – für die Internetverbindung des häuslichen PC. Der D-Kanal dient primär als Steuerkanal. Hier werden die notwendigen Steuerbefehle zwischen dem Vermittlungsrechner und den Endgeräten – zum Beispiel die Signale zum Herstellen und Beenden einer Verbindung oder die Teilnehmerkennung – übertragen. Der D-Kanal bietet damit Hackern die Angriffsfläche, um über eine ISDN-Verbindung eine TK-Anlage zu manipulieren. Solche Manipulationen können beispielsweise dazu führen, daß bestimmte Leistungsmerkmale einer Anlage – für den Betreiber/Nutzer unbemerkt – nach außen hin aktiviert werden. Damit werden u. a. die unbefugte Nutzung (kostenloses Telefonieren), das Abhören von Gesprächen und Räumen sowie das Auslesen der Verbindungsdaten möglich (s. Abb. 9).

Der Nutzer bemerkt die Manipulation dabei nicht:

Zwar erzeugt die TK-Anlage normalerweise bei der Aktivierung sicherheitskritischer Leistungsmerkmale Warnsignale, die den Nutzer auf die Gefahren aufmerksam machen sollen. Sie werden bei solchen Angriffen jedoch durch den Hacker entweder vollständig deaktiviert oder derart manipuliert, daß die Lautstärke und Dauer der Warnsignale auf ein Minimum reduziert werden, so daß eine Aktivierung nicht mehr erkennbar ist.

Auf diese neuartigen Gefahren für die TK-Anlagen – und ihrer Nutzer – habe ich bereits sehr frühzeitig hingewiesen und mich sowohl bei den Herstellern als auch beim BSI um Initiativen für Problemlösungen eingesetzt. Das BSI hat die Entwicklung eines geeigneten Schutzsystems in Auftrag gegeben, das seit Ende 1997 bereit-

steht. Es handelt sich um den sogenannten „D-Kanal-Filter“ – quasi die Firewall für TK-Anlagen –, mit dem es ermöglicht wird, sämtliche auf dem D-Kanal übertragenen Informationen auf ihre Zulässigkeit hin zu überprüfen und damit einen hohen Schutz vor Manipulationen der TK-Anlage zu gewährleisten. Ich begrüße diese Entwicklung sehr und empfehle den Einsatz eines solchen Gerätes in den Dienststellen und Bereichen, in denen besonders schützenswerte Daten verarbeitet werden. Von besonderer Bedeutung ist dies insbesondere dort, wo die TK-Anlage nicht nur die Telefonanbindung einer Dienstelle herstellt, sondern gleichzeitig auch mit dem lokalen Rechnernetz verbunden ist.

10.2.11 Mobiltelefone: „Anrufbeantworter“ abgehört

Auch wenn man sich zu denjenigen zählt, die ohne ein Handy nicht mehr auskommen können, so gibt es doch im alltäglichen Leben immer wieder Gelegenheiten, in denen ein Anruf nicht nur als ungelegen, sondern gar als lästig empfunden wird.

Natürlich kann der Handy-Nutzer in solchen Situationen das Handy einfach ausschalten. Insbesondere bei überwiegend geschäftlich genutzten Handies besteht in aller Regel aber ein Interesse daran zu erfahren, was der Anrufer denn so Wichtiges mitzuteilen hat. Für diese Fälle kann man „den Computer bitten“, den Anruf anzunehmen, eine eventuelle Nachricht aufzuzeichnen und den Handy-Nutzer später zu informieren. Das Gleiche kann der Computer – nämlich der im jeweiligen Mobilfunknetz – auch ohne Bitte tun, wenn das Handy gar nicht im Netz eingebucht, sondern ausgeschaltet ist. Um die Hilfe des Computers zu erhalten, kann man sich bei seinem Mobilfunknetzbetreiber einen Anrufspeicher – auch Mailbox genannt – einrichten lassen. Diese meldet sich (mit einer Sprachansage) beim Anrufer stets dann, wenn der Angerufene nicht im Netz eingebucht oder besetzt ist oder im Moment einfach nicht gestört werden, gleichwohl erreichbar bleiben will.

Sobald der Handy-Nutzer wieder erreichbar ist, informiert ihn der Computer seines Mobilfunknetzes automatisch über zwischenzeitlich eingegangene Anrufe sowie die aufgenommenen Nachrichten, die der Handy-Nutzer auch zu einem ihm passenderen Zeitpunkt abhören kann.

Anfang des Jahres 1998 wurde in der Presse berichtet, daß ungenügende Sicherungsmaßnahmen der Mobilfunknetzbetreiber es Unbefugten vergleichsweise leicht machten, die Mailbox von Handies zu knacken und deren Inhalte – die im übrigen dem Schutz des Fernmeldegeheimnisses unterliegen – abzuhören. Ich habe mich bei den großen Mobilfunknetzbetreibern eingehend über dieses Problem informiert und kann das Ergebnis meiner Recherchen wie folgt zusammenfassen:

Vom eigenen Handy aus kann die Mailbox direkt angewählt und abgefragt werden. Die Sicherheit gegen eine Abfrage durch Unbefugte erscheint hier ausreichend, denn zunächst muß der Nutzer sich gegenüber seinem Handy durch Eingabe einer Kennziffer als Berechtigter ausweisen, dann wird er – genauer: seine im Gerät eingelegte Chipkarte (SIM: **S**ubscriber **I**dentity **M**odule) – vom Netz identifiziert.

Bei Abfrage aus anderen Netzen – vom Festnetz oder aus dem Ausland – wird demgegenüber eine Geheimzahl (PIN: **P**ersonal **I**dentification **N**umber) benötigt. Diese PIN ist meist vierstellig und kann vom Kunden festgelegt werden. Bei einigen Netzbetreibern wird diese voreingestellt, wenn die Mailbox neu eingerichtet wird. Dabei entsteht aber ein Problem, denn ein Netzbetreiber verwendet für seine Millionen Kunden nur wenige unterschiedliche „Start-PIN“, die dann natürlich schnell bekannt werden.

Bekannt ist auch die Regel, nach der ein anderer Netzbetreiber die PIN voreinstellt; sie besteht aus den ersten vier Stellen der Kundennummer – die keineswegs geheim ist!

Wenn der Kunde die ihm von seinem Mobilfunkunternehmen zugeteilte „Start-PIN“ nicht ändert, kann diese von unbefugten Dritten leicht erraten werden. Deshalb sollten diese Unternehmen ihre Kunden nachdrücklich auf dieses Risiko hinweisen und sie auffordern, die PIN zu ändern – auch dann, wenn der Kunde seine Mailbox immer nur vom eigenen Handy abhört und die Geheimzahl somit nie benötigt. Ich bin mit den Netzbetreibern im Gespräch darüber, auf welche Weise hier die Kundeninformation – auch in der Bedienungsanleitung des Netzes und der Computeransage bei der Aktivierung der Mailbox – nachhaltig verbessert werden kann.

Andere Netzbetreiber benutzen keine voreingestellte PIN. Diese muß vielmehr der Kunde bei der Aktivierung der Mailbox selbst festlegen. Der Netzbetreiber erfährt sie gar nicht. Somit besteht die angesprochene Problematik nicht; jedoch kann dann der Kunde bei defektem Handy und vergessener bzw. nicht eingerichteter Geheimzahl seine Mailbox nicht abhören.

Nach meiner Auffassung kann davon ausgegangen werden, daß die Unternehmen ausreichende Sicherungssysteme vorhalten, um die auf den Mailboxen ihrer Kunden gespeicherten Nachrichten vor Zugriffen von unbefugten Dritten zu schützen. Handybesitzer sollten jedoch voreingestellte PIN ändern und ihr Handy nicht zu großzügig von anderen nutzen lassen, denn die Mailbox kann ohne PIN vom Handy aus abgehört werden.

10.2.12 Telekommunikationsdaten ins Ausland geschickt

Mehrere Unternehmen haben sich mit der Frage an mich gewandt, ob und unter welchen Voraussetzungen sie Unternehmen im Ausland mit der Verarbeitung ihrer Telekommunikationsdaten beauftragen dürfen.

Aufgrund der vielfältigen Verflechtungen der in Deutschland tätigen TK-Unternehmen mit ausländischen Telekommunikationsfirmen verwundert es nicht, wenn aus Wirtschaftlichkeitsgründen auf know how, Software- oder Hardwareressourcen, die im ausländischen Partnerunternehmen bereits vorhanden sind, zurückgegriffen werden soll. Beispiele sind u. a. Programme zur Aufbereitung der bei einem Telefonat entstehenden Verbindungsdaten für die Rechnungserstellung sowie Programme zur Erstellung und zum Druck von Kundenrechnungen. Auch der Briefversand der Rechnungen an die deutschen Kunden ist aus dem Ausland oft billiger.

Die Weitergabe der dafür benötigten Daten ist unter bestimmten Voraussetzungen ohne besondere Einwilligung des Kunden zulässig, auch wenn es hierfür keine ausdrückliche spezialgesetzliche Übermittlungsregelung gibt:

Nach § 89 Abs. 2 TKG ist die Nutzung personenbezogener Daten für die dort unter Nrn. 1 bis 3 aufgeführten Zwecke (hierzu zählen auch die o.g. Beispielsfälle) nach Maßgabe einer Rechtsverordnung zulässig, soweit dies für den jeweiligen Zweck erforderlich ist. Eine Rechtsverordnung zu § 89 TKG gibt es noch nicht (siehe hierzu Nr. 10.1.3). Die noch geltende (auf § 10 PTRegG basierende) TDSV enthält zur Zulässigkeit der Übermittlung von Verbindungsdaten zum Zwecke der Auftragsdatenverarbeitung keine speziellen Regelungen. Die Erforderlichkeit als Nutzungsvoraussetzung ist daher nach dem Grundsatz der Verhältnismäßigkeit zu beurteilen, an dem sich auch die Regelungen der zu schaffenden Rechtsverordnung auszurichten hätten. Danach wäre die Weitergabe personenbezogener Daten zur Auftragsdatenverarbeitung zulässig, wenn sie

– im Rahmen der Zweckbestimmung des Vertragsverhältnisses erfolgt und
– soweit sie zur Wahrung berechtigter Interessen der speichernden Stelle erforderlich ist und kein Grund zu der Annahme besteht, daß das schutzwürdige Interesse des Betroffenen an einem Verbot der Übersendung überwiegt.

Die Wahl kostengünstiger Verarbeitungsverfahren z. B. für Abrechnungszwecke liegt sowohl im Rahmen der Zweckbestimmung des Vertrages als auch im Interesse des TK-Dienstleisters.

Schutzwürdige Interessen des Kunden stehen der **Datenweitergabe ins Ausland** zur Auftragsverarbeitung dann grundsätzlich nicht entgegen, wenn der Empfängerstaat ein Datenschutzgesetz besitzt, das auf den Empfänger der Daten anwendbar ist und die datenschutzrechtlichen Grundsätze zur Datenerhebung, zum weiteren Datenumgang und hinsichtlich der Datenqualität sowie in bezug auf die Ansprüche des Betroffenen auf Auskunft usw. berücksichtigt und eine unabhängige Kontrolle der Datenverarbeitung sowie die Zusammenarbeit mit den deutschen Kontrollstellen gewährleistet ist.

Im Hinblick auf die Mitgliedstaaten der EU spielt in diesem Zusammenhang die Datenschutzrichtlinie 95/46/EG vom 24. Oktober 1995 die entscheidende Rolle. Nach Umsetzung der Richtlinie in das nationale Recht der Mitgliedstaaten wird jeder Bürger in einem Mitgliedstaat unionsweit sicher sein können, daß die Übermittlung seiner Daten in andere Mitgliedstaaten dann unproblematisch ist, wenn eine solche Datenübermittlung im eigenen Land zulässig ist.

Allerdings sind bis jetzt nur sechs Mitgliedstaaten ihrer Verpflichtung zur Anpassung ihres Datenschutzrechts an die Vorgaben der Richtlinie nachgekommen (vgl. Nr. 2.1.3). Auch Deutschland hat die Richtlinie noch nicht umgesetzt (s. o. Nr. 2.1.1). Für den Fall von Datenübermittlungen in Mitgliedstaaten, die die Richtlinie noch nicht umgesetzt haben, enthält die Richtlinie allerdings keine gesonderten Regelungen.

Bei der **Weitergabe von Verbindungsdaten in Nicht-EU-Staaten** sind die Voraussetzungen der Artikel 25 und 26 der Richtlinie zu prüfen, d. h. die grundsätzlichen Erfordernisse eines angemessenen Schutzniveaus und gegebenenfalls Ausnahmen und Einschränkungen hierzu (vgl. auch Nr. 2.2.2).

Wegen des in der TDSV enthaltenen Übermittlungsverbotes für Verbindungsdaten dürfen diese jedoch – sowohl innerhalb der EU als auch in Drittstaaten – nur im Rahmen eines Auftragsverhältnisses gem. § 11 BDSG oder an eine unselbständige Stelle derselben Firma weitergegeben werden, d. h. eine Übermittlung im materiellen Sinne bleibt ausgeschlossen, es sei denn, der Beteiligte willigt ein oder eine spezialgesetzliche Erlaubnisnorm greift ein. Dem besonderen Schutzbedürfnis, dem die Verbindungsdaten unterliegen, ist darüber hinaus durch konkrete und abschließende vertragliche Vorgaben zum Datenumgang nach den Vorschriften des TKG und der TDSV Rechnung zu tragen. Die Pflichten des Empfängers und das Weisungsrecht des Auftraggebers sind eindeutig festzulegen.

Verbindungsdaten unterliegen dem besonderen Schutz des Fernmeldegeheimnisses (§ 85 TKG). Deshalb empfehle ich den Unternehmen dringend, bei Verfahren zur Datenfernübertragung an den ausländischen Auftragnehmer besondere technische und organisatorische Maßnahmen zum Schutz vor unberechtigtem Zugriff auf die übertragenen Daten zu treffen. Insbesondere sollten die Daten kryptographisch verschlüsselt übertragen werden.

Im Rahmen der Kontrolle eines Unternehmens, das Verbindungsdaten im Ausland verarbeiten läßt, habe ich festgestellt, daß die vertragliche Absicherung des Datenschutzes im Rahmen des Auftrags nach § 11 BDSG nicht ausreichend war. Insbesondere waren die Vertragsklauseln mit datenschutzrechtlichem Bezug nicht hinreichend konkret. Der schriftliche Auftrag muß in seinen Einzelregelungen zumindest erkennen lassen, welche personenbezogenen Daten zu welchem konkreten Zweck mit welchen DV-Verfahren verarbeitet werden, welchen Schutz diese Daten genießen und welche konkreten organisatorischen und technischen Maßnahmen zu deren Schutz getroffen werden; ein allgemeiner Hinweis auf die Anlage zu § 9 BDSG reicht hier nicht aus. Im einzelnen ausgeführt werden müssen auch die Kontrollrechte des Auftraggebers und die Maßnahmen, die eine wirksame Kontrolle ermöglichen (z. B. Protokollierung, Verarbeitungsstatistiken). Ferner sind etwaige Unterauftragsverhältnisse im einzelnen festzulegen. Bis Redaktionsschluß stand noch nicht fest, wie der Vertrag nachgebessert werden wird.

10.2.13 Der PC als „elektronischer Mülleimer“

Wer kennt sie nicht, die mit unerwünschten Werbesendungen vollgestopften Briefkästen! Verschont werden davon nur die Haushalte, deren Briefkästen einen Aufkleber wie „Bitte keine Werbung!“ tragen.

Diese in vielen Fällen als lästig empfundene Kundenwerbung hat im Zeitalter der weltweiten elektronischen Kommunikation, insbesondere des Internets, eine ganz neue Dimension erhalten. Denn es war so nur eine Frage

der Zeit, bis die Werbebranche auch die Möglichkeiten des Internets für ihre Zwecke entdeckte. Die besondere Problematik liegt dabei darin, daß hier – anders als in konventionellen Verfahren, etwa dem Handzettelverteilen – vollautomatisierte Verfahren eingesetzt werden. Möchte ein Versender elektronischer Werbesendungen möglichst viele E-Mailadressen erreichen, setzt er ein sogenanntes Spiderprogramm ein, daß ähnlich einer Suchmaschine durch das Netz geht und dort sämtliche E-Mailadressen sammelt. Diese Adreßlisten werden dann an interessierte Abnehmer verkauft. Das Versenden erfolgt wiederum mit speziellen Programmen, die gleichlautende E-Mails mit hoher Geschwindigkeit versenden und somit innerhalb äußerst kurzer Zeit einen sehr großen Datenverkehr auslösen, nicht zuletzt auch dadurch, daß sogar nicht mehr gültige und fehlerhafte E-Mailadressen verwendet werden.

Für PC-Nutzer, die über einen Internet-Zugang (über einen Online-Dienst oder einen „Access-Provider“) verfügen, kann dies bedeuten, immer häufiger mit unerwünschter Werbung per E-Mail konfrontiert zu werden.

Damit stellt sich die Frage, wie man sich als Internet-Nutzer davor schützen kann, daß die eigene E-Mailadresse zu Werbezwecken genutzt und der PC im wahrsten Sinne des Wortes zum „elektronischen Mülleimer“ für Werbung per E-Mail wird.

Für PC-Nutzer, die keine Werbung per E-Mail wünschen, besteht grundsätzlich die Möglichkeit, ihre E-Mailadresse in die sogenannte „eRobinson-Liste“ einzutragen, und zwar auf der Website **http://www.eRobinson.com**., die hierzu auch weitere Informationen enthält. Ein entsprechender Eintrag bietet jedoch nicht die Gewähr dafür, keine Werbe-Mails mehr zu erhalten, denn die Nutzung dieser Liste durch die Werbewirtschaft ist lediglich freiwillig. Außerdem zeigt die Erfahrung, daß ausländische Versender von Massenwerbe-Mails die deutsche eRobinson-Liste in aller Regel ignorieren.

Eine andere Möglichkeit, sich gegen ungewollte Werbung dieser Art zu schützen, bietet ein sogenannter **SPAM- oder Anti-SPAM-Filter**, eine besondere Software. SPAM ist ein Begriff, der durch Internet-Nutzer geprägt wurde. Ursprünglich wurde damit ein sehr unappetitliches Frühstücksfleischprodukt aus Schweinefleischresten („**S**pecially **P**repared **A**ssorted **M**eat“) bezeichnet. Inzwischen hat sich die Bezeichnung „SPAM“ im Internet als Synonym für unerwünschte und/oder minderwertige Textbeiträge – insbesondere Werbung per E-Mail – eingebürgert.

In Bereichen der Wissenschaft wird dieses Phänomen mit den Begriffen „**U**nsolicited **B**ulk **E**mail (Unaufgefordert zugesandte Massenpost, UBE)“ oder „**U**nsolicited **C**ommercial **E**mail (Unaufgefordert zugesandte Werbepost, UCE)“ bezeichnet.

Viele Zugangs-Provider – Unternehmen also, die (auch) den Zugang ins Internet ermöglichen – bieten ihren Kunden deshalb sogenannte SPAM- oder Anti-SPAM-Filter an. Diese funktionieren entweder auf der Basis von Listen von bekannten SPAM-Versendern oder von selbstdefinierbaren Stichwörtern zum Ausfiltern von entsprechenden Mails. Auch für den privaten Bereich werden solche Programme vertrieben.

Relativ neu ist der Ansatz, nicht den *Empfang* von SPAM-Mails zu verhindern, sondern den *Versand*. Hierzu werden spezielle Mailserver im Netz angeboten, deren Dienste die Zugangs-Provider in Anspruch nehmen können. Deren besondere Dienstleistung besteht darin, den Versand der E-Mails von SPAM-Versendern länger als nötig in die Länge zu ziehen, so daß das Versenden ihrer Massensendungen über Stunden dauert und die Systeme des Versenders dermaßen belastet werden, daß er diese Mailserver in Zukunft meidet.

Hinzuweisen ist auch darauf, daß bereits elektronische Verzeichnisse auf CD-ROM vertrieben werden, die auch E-Mailadressen enthalten (vgl. auch Nr. 10.3.3). Erfährt dies ein Internet-Nutzer, der mit der eigenen E-Mailadresse nicht auf einer CD vermerkt sein möchte, hat er das Recht, unmittelbar vom Vertreiber der CD-ROM zu verlangen, daß die Eintragung unterbleibt. Dies gilt derzeit aber nur gegenüber Firmen, die in Deutschland ansässig sind. In Zukunft besteht ein solches Unterlassungsrecht auch gegenüber Firmen, die ihren Sitz in anderen EU-Staaten haben. Für Firmen mit Sitz außerhalb der EU, die entsprechende CD-ROM vertreiben, gilt das jeweilige nationale Recht. Hier kann es schwer bis unmöglich werden, eine Löschung in einem solchen elektronischen Verzeichnis durchzusetzen.

10.3 Der Kunde nimmt seine Rechte wahr

10.3.1 Kein Fernmeldegeheimnis bei Rechnungseinwendungen?

„Soviel habe ich niemals vertelefoniert!“ So lautet nicht selten der Kommentar, wenn die monatliche Telefonrechnung kommt. Wie jeder, der für erbrachte Leistungen eine Zahlung verlangt, muß in solchen Fällen auch das TK-Unternehmen die zunächst pauschalierte Rechnung detaillieren und die Forderung auf diese Weise näher begründen.

Die TK-Unternehmen teilen hierzu dem Kunden – ähnlich wie beim EVN – die Verbindungsdaten (Zeitpunkt, Dauer, angerufene Nummer) der entgeltpflichtigen Gespräche mit und geben ihm somit die Möglichkeit zur Überprüfung der Rechnung. Damit erhält der Kunde aber nicht nur Kenntnis über die Daten der eigenen Gespräche, sondern auch derjenigen Personen, die mit ihm das Telefon genutzt haben, also z. B. der Ehefrau, der (minder- und volljährigen) Kinder oder der Schwiegermutter. Aber auch deren Telefonate unterliegen dem Schutz des Fernmeldegeheimnisses!

Durch den Hinweis eines Bürgers ist mir bekanntgeworden, daß ein großes TK-Unternehmen bei Streitigkeiten über die Höhe von Verbindungsentgelten dem Kunden die Verbindungsdaten mitteilt, ohne daß die Mitbenutzer des Anschlusses hierin eingewilligt haben.

Das TK-Unternehmen leitet die Befugnis für dieses Vorgehen aus § 6 Abs. 7 Satz 5 TDSV ab, wo es lediglich heißt: *„Dem Kunden dürfen ... die ... nach dem Versand*

der Rechnung gespeicherten Daten mitgeteilt werden, wenn er Einwendungen gegen die Höhe der Verbindungsentgelte erhoben hat." Explizite Regelungen zum Schutz der Mitbenutzer enthält die Vorschrift nicht. Dies darf im Rahmen einer zweckorientierten Auslegung der TDSV nicht dazu führen, die Mitbenutzer hinsichtlich des Fernmeldegeheimnisses schutzlos zu stellen.

Die Verordnungsermächtigung für die TDSV enthält das Gesetz über die Regulierung der Telekommunikation und des Postwesens (PTRegG) vom 14. September 1994. Gemäß § 10 Abs. 2 Nr. 3a PTRegG dürfen Unternehmen und Personen, die Telekommunikationsdienstleistungen erbringen oder an der Erbringung solcher Dienstleistungen mitwirken, einem Kunden auf schriftlichen Antrag Verbindungsdaten nur *„unter Wahrung des in der Rechtsverordnung zu regelnden Schutzes von Mitbenutzern"* mitteilen. Der Gesetzgeber hat die besondere Verpflichtung des Anschlußinhabers gegenüber den Mitbenutzern dadurch betont, daß er eine wortgleiche Regelung in § 89 Abs. 2 Ziffer 3a TKG aufgenommen hat.

Durch die TDSV wird das Fernmeldegeheimnis von Mitbenutzern lediglich geschützt, wenn der Auftrag für einen EVN erteilt wird (§ 6 Abs. 7 Satz 2 TDSV) – also für künftige Verbindungen; sie müssen hier vorher vom Auftraggeber informiert werden. Für die (nachträgliche) Bekanntgabe von Verbindungsdaten bei Entgeltstreitigkeiten enthält die TDSV jedoch keinerlei Schutzvorschrift. Angesichts der Schutzbedürftigkeit der Daten, die dem Fernmeldegeheimnis unterliegen, ist dies ein gravierendes Defizit, das für die Mitbenutzer zu einer Verletzung ihres Rechts auf informationelle Selbstbestimmung führen kann. Dies muß durch eine datenschutzgerechte Anwendung von § 6 Abs. 7 Satz 5 TDSV wegen der höherrangigen Norm des § 10 Abs. 2 Ziffer 3a PTRegG bzw. § 89 Abs. 2 Ziffer 3a TKG vermieden werden.

Eine Bekanntgabe von Verbindungsdaten an den Kunden im Rahmen von Rechnungsstreitigkeiten darf daher nur mit der **Einwilligung der Mitbenutzer** des Telefonanschlusses im Haushalt erfolgen.

Leider hat das bis Ende 1997 zuständige BMPT meine Rechtsauffassung nicht geteilt. Von dort wurde mir mitgeteilt, daß zwar der in § 10 Abs. 2 Nr. 3a PTRegG und § 89 Abs. 2 Nr. 3a TKG festgeschriebene Schutz von Mitbenutzern – ungeachtet der fehlenden Erwähnung im Wortlaut des § 6 Abs. 7 S. 5 TDSV – zu wahren sei. Dieser Schutz erfordere allerdings keine ausdrückliche Einwilligung der Mitbenutzer eines Anschlusses in die Weitergabe der Verbindungsdaten an den Anschlußinhaber. Hier müsse eine schriftliche **Erklärung des Anschlußinhabers**, daß er seine Mitbenutzer entsprechend informiert habe bzw. informieren werde, ausreichend sein. Nachdem der Mitbenutzer seine Telefonate geführt hat, nützt ihm eine Information über die bevorstehende Mitteilung der Verbindungsdaten wegen Rechnungsstreitigkeiten aber nichts mehr.

Ich werde mich im Rahmen der anstehenden Änderung der TDSV für eine Regelung einsetzen, die klarstellt, daß bei Entgeltstreitigkeiten die Verbindungsdaten der Mitbenutzer des Telefons nur weitergegeben werden dürfen, wenn deren Einwilligung vorliegt. Anders kann eine mögliche Verletzung des informationellen Selbstbestimmungsrechts der Mitbenutzer nicht vermieden werden.

10.3.2 Probleme mit Kundenverzeichnissen und Auskunftsdiensten

Immer wieder erhalte ich Schreiben von Bürgern, die sich darüber beklagen, daß sie z. B. mit Namen, Anschrift und Beruf in einem gedruckten oder elektronischen öffentlichen Kundenverzeichnis eingetragen sind oder diese Daten von einem telefonischen Auskunftsdienst weitergegeben werden, obwohl sie dies nicht beantragt haben. Durch das TKG wurde dem Kunden das Recht gegeben, selbst zu bestimmen, ob und in welcher Form er in ein Kundenverzeichnis eingetragen oder beauskunftet wird (§ 89 Abs. 8, 9 TKG). Nach der früheren Regelung des „Zwangseintrags" – der 1991 aufgehoben wurde – und der damals bestehenden Möglichkeit, Widerspruch gegen einen Eintrag einzulegen, dürfen heute nur noch die Einträge in die Verzeichnisse aufgenommen werden, die vom Kunden ausdrücklich beantragt wurden.

Es gibt oft sehr wichtige Gründe, warum sich jemand entscheidet, nicht einmal mit einem verkürzten Eintrag in einem öffentlichen Kundenverzeichnis vertreten zu sein. Es ist nicht nur der Wunsch, keine störenden Werbesendungen oder -anrufe zu erhalten. So wurden mir Fälle mitgeteilt, in denen Frauen nicht in ein Verzeichnis eingetragen werden wollten, weil sie Angst vor ihrem Ex-Mann oder Ex-Freund haben. In einigen Fällen erfolgte dann doch ein Eintrag, teilweise sogar mit Anschrift. Dies führte dann zu konkreten Belästigungen und Bedrohungen, weil dadurch der Aufenthaltsort oder zumindest die Telefonnummer bekannt geworden waren.

Ich habe diese sich häufenden Beschwerden zum Anlaß genommen, bei einem großen TK-Unternehmen nachzuprüfen, wie die gesetzlichen Vorgaben im Arbeitsablauf des Unternehmens umgesetzt werden, angefangen von der Entgegennahme der Aufträge über die Bearbeitung bis hin zur Information des Kunden.

Dabei mußte ich feststellen, daß den Mitarbeitern in den verschiedenen Arbeitseinheiten oft nicht alle Wahlmöglichkeiten der Veröffentlichung bekannt waren. Dies ist umso bedauerlicher, als viele dieser Mitarbeiter die Kunden beraten sollen und gerade diese Vorschriften für den Schutz des Persönlichkeitsrechts wichtig sind. Die mangelnde Kenntnis ist darauf zurückzuführen, daß die Mitarbeiter nicht hinreichend geschult werden. Dem kann durch eine ausreichende Fortbildungsmaßnahme begegnet werden, die ich dem Unternehmen empfohlen habe.

Eine weitere Fehlerquelle bei der Bearbeitung der Kundenwünsche lag im Bereich der verwendeten Computerprogramme. So gab es im Zusammenhang mit dem Eintragungswunsch eine Vorbelegung in der Bearbeitungsmaske auf dem Monitor dergestalt, daß Name und Anschrift des Kunden zunächst für die Telefonbucheintra-

gung vorgesehen waren. Dies kann bei großer Arbeitsbelastung der Mitarbeiter zu einer Fehlerquelle werden, wenn vergessen wird, den Kunden auf diesen Punkt speziell anzusprechen bzw. hierzu anzuschreiben.

Ich habe das betroffene Unternehmen aufgefordert, die festgestellten Mängel zu beheben, soweit dies technisch möglich ist. Es bleibt aber festzuhalten, daß die meisten mir vorliegenden Eingaben in diesem Bereich durch Arbeitsfehler bedingt waren (s. dazu auch Nr. 10.2.1). Hier kann nur durch angemessene und regelmäßige Aus- und Fortbildungsmaßnahmen Abhilfe geschaffen werden.

10.3.3 Das Telefonbuch auf CD-ROM: Immer wieder Ärger

Auch in meiner Dienststelle ist die CD-ROM unverzichtbarer Informationsträger geworden. Das gilt insbesondere für das „elektronische Telefonbuch“, auf das jeder Mitarbeiter von seinem PC aus zugreifen kann. Nach wie vor muß ich jedoch feststellen, daß keineswegs alle Menschen, die in solchen Datenbanken eingetragen sind, darüber glücklich sind. Da gibt es diejenigen, die in überhaupt keinem Verzeichnis – weder in einem gedruckten noch in einem elektronischen – eingetragen sein möchten. Andere haben nichts gegen die Eintragung in ein gedrucktes Verzeichnis, wie z. B. das „normale“ Telefonbuch, lehnen die Eintragung in ein elektronisches Verzeichnis, wie die CD-ROM, jedoch strikt ab. Ich habe hierüber bereits ausführlich in meinem 16. TB berichtet (Nr. 5.10 und Nr. 10.4.5).

Tatsächlich betreffen die meisten Beschwerden von Bürgern das Telefonbuch auf CD-ROM, das inzwischen von mehreren Unternehmen herausgegeben wird. Dabei lautet die Beschwerde meistens, sie seien im „elektronischen Telefonbuch“ eingetragen, obwohl sie ihrem TK-Unternehmen keine Einwilligung zur Weitergabe ihrer Daten an den Herausgeber erteilt hätten. Einige haben dies ihrem TK-Unternehmen sogar ausdrücklich untersagt.

Leider muß ich den Bürgern in solchen Fällen stets mitteilen, daß die Datenschutzaufsicht über die mir bekannten privaten Herausgeber eines elektronischen Telefonbuches außerhalb meiner Zuständigkeit liegt: Die Datenschutzaufsicht über die in Deutschland ansässigen Herausgeber liegt bei den Aufsichtsbehörden der Länder. An diese muß ich die Beschwerdeführer zumeist verweisen. Leider kann auch die Aufsichtsbehörde dem Beschwerdeführer oft nicht helfen. So hat ein großer Anbieter eines Telefonbuches auf CD-ROM den Sitz seines Unternehmens von Deutschland in das zu Österreich gehörende Kleinwalsertal verlegt, nachdem es in Deutschland Gegenstand massiver – auch datenschutzrechtlicher – Kritik geworden war. Auch Österreich hat ein hohes Datenschutzniveau. Jedoch sind dort für den privaten Bereich die Gerichte zuständig, bei denen bisher in der Sache keine Klagen anhängig sind. Die europäische Datenschutzrichtlinie 95/46/EG vom 24. Oktober 1995 (s. o. Nr. 2.1.1), die bedauernswerterweise während der dreijährigen Umsetzungsfrist weder in Österreich noch in Deutschland rechtzeitig in nationales Recht umgesetzt wurde (s. o. Nr. 2.1.1.1 und Nr. 2.1.3), bildet die rechtliche Antwort auf die Herausforderungen des informationellen Großraums Europa. Nach erfolgter Umsetzung der Richtlinie in allen Mitgliedstaaten der Europäischen Union wird der europäische Binnenmarkt auch hinsichtlich des Datenschutzes verwirklicht sein, was bedeutet, daß der Umgang mit personenbezogenen Daten nicht gleichzeitig in einem Mitgliedstaat zulässig und in einem anderen Mitgliedstaat unzulässig sein kann. Sollten sich dann gleichwohl Unterschiede zwischen den Rechtsvorschriften oder der Praxis der Mitgliedstaaten ergeben, die die Gleichwertigkeit des Datenschutzes in der Gemeinschaft beeinträchtigen könnten, wird die Datenschutzgruppe nach Artikel 29 der Richtlinie die Europäische Kommission hierüber in Kenntnis zu setzen haben, die – ihrerseits unterstützt von dem Ausschuß nach Artikel 31 – die entsprechenden Maßnahmen zu treffen hat.

In meiner Zuständigkeit liegt es allerdings zu überprüfen, ob der Wunsch des Kunden von seinem TK-Unternehmen berücksichtigt wurde. Denn seit dem Inkrafttreten des Telekommunikationsgesetzes (TKG) im August 1996 darf ein Telefonkunde überhaupt nur dann in öffentliche Verzeichnisse eingetragen werden, wenn er dies ausdrücklich beantragt hat; ein „nicht erfolgter Widerspruch“ ist hier nicht ausreichend (§ 89 Abs. 8 TKG). Dabei kann er auch entscheiden, ob er nur ins gedruckte Telefonbuch, nur in ein elektronisches Verzeichnis oder aber in beide eingetragen werden möchte. Ich habe feststellen können, daß die TK-Unternehmen dem grundsätzlich Rechnung tragen. Wenn es dennoch zu Fällen kommt, in denen ein Telefonkunde entgegen seinem Votum ins Telefonbuch eingetragen wird, so hat es sich bisher stets um Arbeitsfehler gehandelt, die – zu Recht oder zu Unrecht – als in einem Massengeschäft unvermeidbar bezeichnet werden (s. o. Nr. 10.2.1.). Gleichwohl müssen die TK-Unternehmen auch bei der Bewältigung eines Massengeschäftes durch organisatorische und technische Maßnahmen sicherstellen, daß das Recht des Kunden auf informationelle Selbstbestimmung auch bei besonderer Arbeitsbelastung und erhöhtem Streß sichergestellt wird. Hierzu habe ich ein großes TK-Unternehmen nachdrücklich aufgefordert und sehe mit Interesse den ergriffenen Maßnahmen entgegen.

10.3.4 Nachlässiger Umgang mit Kundendaten

Datenschutzregelungen mögen von besonders serviceorientierten Unternehmen und auch von einzelnen Kunden gelegentlich als unnützer Formalismus empfunden werden. Ein aktuelles Beispiel aus Dresden zeigt jedoch, wie übertriebenes Bestreben nach vorgeblich besonders kundenfreundlichem Verhalten dazu führen kann, daß wichtige Kundeninteressen in einer Weise verletzt werden, die bei den Betroffenen – sofern ihnen der Vorgang bekannt würde – alles andere als ein positives Bild des Unternehmens entstehen ließen.

Mitarbeitern einer Dresdener Zeitung war es gelungen, in mehreren Verkaufsstellen sowie bei der Störungsannahme und der Rechnungsstelle eines großen TK-Unternehmens Auskünfte über Kundendaten – Name,

Anschrift, Telefonnummer – zu erlangen, ohne daß in irgendeiner Form überprüft worden war, ob sie zum Erhalt dieser Auskünfte legitimiert waren.

Dies ist keineswegs eine „läßliche Sünde“, denn das TKG hat den Kunden von TK-Unternehmen hier sehr weitgehende Rechte eingeräumt: Sie können selbst bestimmen, ob sie ihre Daten überhaupt – und gegebenenfalls welche – zur Veröffentlichung in einem Telefonverzeichnis oder zur Auskunfterteilung im Rahmen der Telefonauskunft freigeben. Häufig wird nur die Veröffentlichung des Nachnamens, des ersten Buchstabens des Vornamens sowie der Telefonnummer gewünscht – so z. B. von vielen Frauen – oder es wird gänzlich auf die Veröffentlichung und Auskunftserteilung verzichtet – z. B. von Prominenten oder von Personen, die sich konkret von anderen belästigt oder bedroht fühlen.

In einer Verkaufsstelle des TK-Unternehmens war von dem Mitarbeiter, nachdem ihm die Rufnummer einer Kundin genannt worden war, deren Adresse nicht im Telefonbuch stand, der vollständige Datensatz dieser Kundin auf dem frei einsehbaren Computerbildschirm aufgerufen worden, so daß die Mitarbeiter der Zeitung die komplette Adresse lesen konnten. Nach einem Ausweis oder einer Vollmacht war nicht gefragt worden. In einer anderen Filiale wurden den „kundenfreundlichen“ Mitarbeitern des TK-Unternehmens Adreßangaben unter dem Vorwand entlockt, die letzte Rechnung sei – wohl aufgrund eines Adreßfehlers – nicht angekommen. Auch hier ließ man sich weder einen Ausweis vorlegen noch wurde die Identität des vermeintlichen Kunden in sonstiger Weise geprüft. Nach Angaben der Zeitung waren auf ähnlich leichte Weise telefonische Auskünfte von der Störungsstelle und der Rechnungsstelle des Unternehmens zu erhalten, wobei in einem Fall sogar ohne vorherige Legitimationsprüfung die Höhe der letzten Telefonrechnung mitgeteilt worden sei.

Das betroffene TK-Unternehmen, das ich zu dem Pressebericht der Zeitung um Stellungnahme gebeten hatte, bedauert die Vorkommnisse. Die Mitarbeiter des Unternehmens sind aus Anlaß der geschilderten Vorfälle nochmals für den direkten Kundenkontakt geschult worden und besonders darauf hingewiesen worden, daß auch bei „souveränem“ Auftreten von Kunden der eindeutigen Identifikation des Besuchers oder Anrufers besondere Aufmerksamkeit zu widmen ist, wenn dieser kundenbezogene Auskünfte verlangt. Darüber hinaus sollen in sämtlichen Verkaufsfilialen des Unternehmens die Computerbildschirme in den für Kunden zugänglichen Räumen sichtgeschützt aufgestellt werden.

10.3.5 „Vor dem Reden Gehirn einschalten“: Auskünfte über Schulden von TK-Kunden an Banken

Ein Bürger stellte fest, daß eine Überweisung, mit der er seine Telefonrechnung bei einem großen TK-Unternehmen begleichen wollte, nicht in seinen Kontoauszügen auftauchte. Er sprach daraufhin bei der zuständigen Filiale seiner Bank vor und versuchte, die Sache zu klären.

Die Klärung gestaltete sich dann etwas schwieriger, denn *„... nach längerer Unterhaltung mit dem Filialleiter griff dieser zum Telefon und wählte die Kundenbuchhaltung des Telekommunikationsunternehmens an. ... Die Dame am anderen Ende der Leitung plauderte über meinen Kontostand und daß schon eine Mahnung zu mir unterwegs sei.“*

Irritiert und verärgert über diesen Vorgang fragte er bei mir an, wie das Verhalten des TK-Unternehmens datenschutzrechtlich zu bewerten sei.

Von dem TK-Unternehmen erfuhr ich, daß solche Anfragen von Banken nur selten vorkommen und diese sich dabei in der Regel danach erkundigen, ob von ihnen durchgeführte Überweisungen auch tatsächlich einem bestimmten Kundenkonto gutgeschrieben wurden. Die Mitarbeiter des Unternehmens hätten sich aber zu vergewissern, ob der Anrufer wirklich derjenige ist, der er vorgibt zu sein.

Die Mitarbeiter führen diese Identifikation anhand bestimmter Kriterien – von deren datenschutzrechtlicher Zulässigkeit ich mich überzeugt habe – durch. Diese Vorgehensweise gilt nicht nur bei Anfragen von Banken, sondern wird auch bei Anfragen von Kunden angewandt. Dabei beschränken sich die Auskünfte des Unternehmens auf die Übermittlung von personenbezogenen Daten, die **je nach Einzelfall** für die Entgeltabrechnung erhebliche Umstände enthalten, was durch die Vorschrift des § 6 Abs. 2 TDSV gedeckt ist. Das Unternehmen räumte in diesem Zusammenhang ein, daß es sich im Einzelfall des anfragenden Bürgers um eine unzulässige Datenübermittlung an Dritte gehandelt hat, *„da die Kenntnis über den Kontostand des Bürgers und die Tatsache, daß bereits eine Mahnung versandt wurde, in diesem Zusammenhang eben nicht einen für die Entgeltabrechnung erheblichen Umstand darstellt“.* Zur Vermeidung solcher Arbeitsfehler werde jedoch von den Führungskräften des Unternehmens im Rahmen der betrieblichen Fortbildung auf die Brisanz dieser Aspekte kontinuierlich hingewiesen.

Datenschutzrechtlich ist das Verfahren bei der telefonischen Erteilung von Auskünften an Banken zur ordnungsgemäßen Abrechnung der Entgelte nicht zu bemängeln, wenn dabei nur die **erforderlichen Angaben** den **Berechtigten** gemacht werden, wie es die unternehmensinternen Regelungen vorschreiben. Ich werde die Mitteilung des Bürgers jedoch zum Anlaß nehmen, zu kontrollieren, inwieweit die entsprechenden Regelungen Eingang in den Arbeitsalltag der zuständigen Mitarbeiter des Unternehmens – aber auch anderer TK-Unternehmen – gefunden haben.

10.3.6 Schlupfloch geschlossen: Bessere Zugriffsprotokollierung bei Datenbanken

Eine Bürgerin teilte mir folgenden Sachverhalt mit:

Sie habe nach ihrer Scheidung bereits mehrfach die Wohnung gewechselt, ihre jeweils neue Telefonnummer nicht ins Telefonbuch eintragen lassen und diese auch nicht für die Auskunft freigegeben. Trotzdem habe ihr geschiedener Ehemann, ein Polizist, zu dem sie jeglichen Kontakt abgebrochen habe, bereits kurz nach jedem Umzug ihre Rufnummer und die neue Adresse in Erfahrung

gebracht. In diesem Zusammenhang äußerte sie die Vermutung, daß er seine Zugehörigkeit zur Polizei in Verbindung mit „freundschaftlichen Diensten“ von Telekom-Mitarbeitern ausgenutzt haben könne.

Für die Arbeit der Polizei und anderer Sicherheitsbehörden ist es oftmals wichtig zu wissen, wer der Anschlußinhaber einer bestimmten Telefonnummer ist oder welche Telefonnummer eine bestimmte Person hat und wo sich der Anschluß befindet – auch wenn der Anschluß nicht im Telefonbuch eingetragen ist. Nach §§ 89 Abs. 6 und 90 TKG haben die Telekommunikationsunternehmen derartigen Auskunftsersuchen zu entsprechen. Über das Verfahren, nach welchem die Deutsche Telekom AG (DTAG) gegenwärtig diese Auskunftsersuchen entgegennimmt, bearbeitet und beantwortet, habe ich mich bei einem der insgesamt zehn Vertriebsteams für Behörden mit Sicherheitsaufgaben (VT-BS) der DTAG informiert (s. auch 16. TB Nr. 10.4.14).

Um den berechtigten Stellen die gewünschten Auskünfte geben zu können, greifen die Bearbeiter der Auskunftsersuchen auf Datenbanksysteme der DTAG zu und entnehmen diesen die erforderlichen Angaben. Da diese Datenbanksysteme nicht ausschließlich für die VT-BS konzipiert wurden, sondern auch vielen anderen Arbeitsgebieten innerhalb der DTAG (z. B. Auftragsmanagement, Buchdienst) zur Verfügung stehen, ist auch tausenden anderen Mitarbeitern – für ihre jeweilige Aufgabenerledigung – der Zugriff auf diese Datenbanken gestattet. Die Zugriffe müssen protokolliert werden (Nrn. 5 und 7 der Anlage zu § 9 Satz 1 BDSG). Anhand der Protokolldaten kann dann festgestellt werden, wer wann – lesend oder schreibend – auf welche Daten zugegriffen hat.

Da beim zuständigen VT-BS hinsichtlich der Daten der Bürgerin keine Anfragen berechtigter Bedarfsträger vorlagen, hätte mit Hilfe eines solchen Protokolls grundsätzlich die Möglichkeit bestanden, die Zugriffe auf den Datensatz der Bürgerin zu überprüfen. Wegen des inzwischen eingetretenen Zeitablaufs – die Protokolldaten können aus Kapazitätsgründen nur jeweils 16 Tage aufbewahrt werden – schied die Möglichkeit einer entsprechenden Recherche jedoch aus, so daß der Bürgerin lediglich mitgeteilt werden konnte, daß keine Anhaltspunkte dafür vorliegen, die ihre Vermutung bestätigen oder entkräften. Jedoch schon während meiner Kontrolle bei dem zuständigen VT-BS ergaben sich Anhaltspunkte dafür, daß die Datenbankzugriffe nicht lückenlos protokolliert werden.

Aus einer Stellungnahme der Telekom ging dann auch hervor, daß sich die Protokollierung nur auf etwa 90% der Zugriffe **aller** der oben erwähnten Datenbanknutzer – also neben dem VT-BS vor allem dem Auftragsmanagement und dem Buchdienst – erstreckt, wobei sie von rund 20 000 Zugriffen pro Sekunde ausging. Etwa 10% der Zugriffe erfolgen über sog. Seiteneingänge der Datenbanksysteme und werden von der Protokollierung nicht erfaßt, was stündlich etwa 7 Millionen Zugriffe betraf.

Angesichts dieses Umfangs an nichtprotokollierten Zugriffen ist es durchaus wahrscheinlich, daß zwar autorisierte, jedoch nicht dem konzipierten Zweck dienende Zugriffe auf die Datenbestände – auch solche im Rahmen von „Freundschaftsdiensten“ – unentdeckt bleiben. Die Telekom wies von sich aus darauf hin, daß Recherchen zur Erkennung unberechtigter Zugriffe bereits unternommen worden seien. Deren Aussagefähigkeit dürfte allerdings in Anbetracht des Anteils an nichtprotokollierten Zugriffen m.E. nur mangelhaft gewesen sein.

Nachdem ich der Telekom mitgeteilt hatte, daß diese Art der Protokollierung mit einer derart hohen „Ausfallquote“ nicht den Vorgaben des § 9 BDSG entspricht, informierte sie mich, daß sie durch arbeitsorganisatorische Maßnahmen und programmtechnische Veränderungen der Zugriffsprotokollierung seit Mai 1998 eine lückenlose Protokollierung der Zugriffe auf die Datenbanken gewährleisten könne. Ich werde dem zu gegebener Zeit nachgehen.

10.3.7 Mit der „Sprechenden Kundennummer“ ins Jahr 2000?

Auch im Berichtszeitraum beschwerten sich wieder Kunden der DTAG bei mir über deren Abrechnungsverfahren, bei dem die Telefonnummer der Kunden – in Gestalt der sog. Fernmeldekontonummer (FKTO) – als Kundennummer genutzt wird. Hierdurch erlangt die kontoführende Bank im Rahmen des Abbuchungsverfahrens Kenntnis von der Telefonnummer. Datenschutzrechtlich ist dies eine Übermittlung personenbezogener Daten, wofür die TDSV keine Erlaubnis enthält. Besonders solche Kunden, deren Geheimnummer/Telefonnummer nicht im Telefonbuch steht, kritisieren dieses Verfahren.

Ich weise die DTAG hierauf seit Jahren hin (zuletzt 16. TB Nr. 35 – Nr. 8) und dränge auf Änderung des auch von ihr selbst als datenschutzrechtlich problematisch beurteilten Verfahrens. Eine Änderung wurde zwar schon Anfang 1995 für die damals geplante Einführung eines neuen Fakturierungssystems – zunächst für Anfang 1996 – in Aussicht gestellt. Dieser Termin wurde allerdings immer wieder verschoben. Als Grund für die lange Dauer der Umstellung wurde mir die außerordentliche Komplexität des Abrechnungsverfahrens bei mehr als 40-Millionen monatlich zu erstellenden Rechnungen und den dabei zu berücksichtigenden vielfältigen Sonderfällen genannt.

Auf Nachfrage erklärte die DTAG im Frühjahr 1998, daß die Umstellung der FKTO auf eine von der Telefonnummer unabhängige Kundennummer bis spätestens September 1998 für ca. 90% aller Kunden und spätestens bis zum 30. Juni 1999 vollständig abgeschlossen sei.

Der DTAG habe ich daraufhin mitgeteilt, daß ich den Abschluß der Umstellung bis 30. Juni 1999 als zu langfristig beurteile, zumal nicht nachvollziehbar ist, warum für die Umstellung der letzten 10% der FKTO nochmals 9 Monate benötigt werden. Ich habe in diesem Zusammenhang auch gebeten, die Umstellung der FKTO von Privatkunden – insbesondere von denjenigen, die einer Veröffentlichung ihrer Daten in öffentlichen Kundenverzeichnissen widersprochen haben – zeitlich vorzuziehen.

Die DTAG hat diese Bitte abgelehnt und die Kritik an der Verfahrensdauer, die sich immerhin über vier Jahre erstreckt, zurückgewiesen. Sie hat in diesem Zusammenhang allerdings auch erläutert, daß man nicht mehr an der zunächst beabsichtigten Reparatur des alten Systems festhalte, sondern ein vollständig neues Abrechnungssystem einführen werde. Deshalb gestalteten sich die entsprechenden Softwareanpassungen, die nicht nur einfach ein Auswechseln der FKTO gegen die Kundennummer enthalten, sondern komplette Abrechnungsstrukturen änderten, sehr zeitaufwendig und schwierig. Die auf den ersten Blick unverhältnismäßig lange Restzeit der Umstellung der verbleibenden 10% aller FKTO ergebe sich daraus, daß erst ab 1999 die Software so programmiert sei, daß sie alle Sonderfälle aus den alten Abrechnungssystemen berücksichtigen könne. Eine vorrangige Umstellung der FKTO derjenigen Kunden, die einer Veröffentlichung ihrer Daten in öffentlichen Kundenverzeichnissen widersprochen haben, sei leider nicht möglich.

Ich werde die Entwicklung mit großer Aufmerksamkeit verfolgen und auf den Verfahrensfortschritt drängen.

10.3.8 Die T-Net-Box der Telekom

Telefonanrufbeantworter werden häufig und gerne genutzt. Angesichts des vielfältigen Angebotes ist oftmals bereits die Auswahl des richtigen Gerätes ein Problem. Oft geben Bedienung und Störanfälligkeit Grund zum Ärgern. Mit Interesse werden daher die Kunden der Deutschen Telekom AG ein Faltblatt mit dem Titel *„Nie wieder einen Anruf verpassen“* gelesen haben, das sie im Sommer 1997 als Beilage zu ihrer Telefonrechnung erhielten.

Hierin wurde den Kunden die sogenannte T-Net-Box angeboten, die über alle Funktionen eines Anrufbeantworters verfügt, *„aber noch viel mehr kann“*. Das Angebot richtete sich an jeden Telekom-Kunden, der ein „mehrfrequenzwahlfähiges“ Telefon – beim Wählen sind hier unterschiedlich hohe Töne zu hören – oder einen ISDN-Anschluß hat. Der Kunde konnte sich sofort von zu Hause aus eine T-Net-Box einrichten und betreiben. Dem Faltblatt war dazu eine Kurzanleitung zu entnehmen; nach dem danach erfolgten Einrichten der T-Net-Box wurde eine umfangreiche Bedienungsanleitung übersandt.

Abgesehen von den inzwischen hinzugekommenen weiteren Leistungsmerkmalen der T-Net-Box – so besteht jetzt auch die Möglichkeit, jedem zum Haushalt gehörenden Teilnehmer eine individuelle Box einzurichten oder über die Box Faxsendungen zu empfangen – funktioniert die T-Net-Box wie ein herkömmlicher Anrufbeantworter. Der einzige Unterschied besteht darin, daß sie sich körperlich nicht in der direkten Verfügungsgewalt des Nutzers befindet, sondern Bestandteil eines IT-Systems der Telekom ist.

In der Regel legt der Besitzer eines Anrufbeantworters Wert darauf, daß die auf diesem gespeicherten Nachrichten nur einem von ihm bestimmten Personenkreis zur Kenntnis gelangen können. Ein Anrufer erwartet ebenso, daß seine Nachricht nur dem zur Kenntnis gelangt, für den sie bestimmt ist. Wer also einen Anrufbeantworter nutzt, schützt ihn vor unbefugtem Zugriff, indem er etwa die Wohnung bei Abwesenheit verschließt und den Anrufbeantworter durch dafür vorgesehene hard- und softwaretechnische Einrichtungen schützt.

Da sich die T-Net-Box nicht in der Wohnung des Nutzers befindet, müssen an die Sicherheit ihres Betriebes entsprechend höhere Anforderungen gestellt werden. Entscheidend für die sichere Nutzung einer T-Net-Box ist eine persönliche Identifikationsnummer (PIN), die der künftige Nutzer bei ihrer Einrichtung vorgibt. Die PIN ist von Wirkungsweise und Bedeutung vergleichbar mit einer PIN zur Nutzung von Kreditkarten oder mit einem Paßwort, das den Zugang zu – z. B. auf Personalcomputern gespeicherten – Daten und Programmen eröffnet.

Deshalb habe ich die Telekom aufgefordert, die Kunden in den nächsten Ausgaben des Faltblattes und der Bedienungsanleitung zur T-Net-Box eingehender als bisher über die mit der Bildung der PIN verbundenen Sicherheitsaspekte zu informieren. Diese sind leider nicht – wie die Telekom in einer ersten Reaktion meinte – „breiten Bevölkerungsschichten“ bekannt. Bei Beratungs- und Kontrollbesuchen in anderem Zusammenhang treffen meine Mitarbeiter immer wieder geringstellige PIN u. ä. an. Zudem sind viele Systeme auch noch so gestaltet, daß sie nur eine geringe Stellenzahl zulassen. Die PIN für die T-Net-Box muß erfreulicherweise mindestens 4 Stellen lang sein und kann bis zu 10 Stellen umfassen. Leider werden im Faltblatt und in der Bedienungsanleitung jedoch nur Beispiele mit vierstelliger PIN gezeigt. Deshalb ist es hier erforderlich, in künftigen Fassungen des Faltblattes und der Bedienungsanleitung auf dieses Problem hinzuweisen, z. B. durch eine Formulierung wie: „Das Risiko, eine PIN zu erraten oder auszuforschen, nimmt mit der Anzahl der für die Bildung der PIN verwendeten Ziffern ab". Die Telekom hat mir schließlich zugesagt, diesen Text in die nächste Ausgabe des Faltblattes einzuarbeiten. Dieses Faltblatt *„Der Anrufmanager ist da“* liegt seit dem Spätsommer 1998 vor, unterscheidet sich jedoch – jedenfalls in dieser Hinsicht – nicht von seinem Vorgänger. Dies ist für mich Grund genug, die Diskussion mit der Telekom zu Sicherheitsaspekten bei der Nutzung der T-Net-Box verstärkt fortzuführen.

In einem derart sensiblen Bereich ist es auch wichtig, den Mitarbeitern in Arbeitsanweisungen sachgerechte Vorgaben für eine sicherheitsgerechte Aufgabenerledigung zu machen. Ein in diesen Arbeitsanweisungen zu regelnder Aspekt betrifft die Tätigkeit der Systemverwalter. Zwar hat die Telekom mitgeteilt, daß ein Zugriff auf die aufgesprochenen Nachrichten in der T-Net-Box nicht möglich ist, weil sie verschlüsselt abgespeichert werden. Dabei gehe ich davon aus, daß das für die von den Kunden vergebenen PIN auch zutrifft. Nun sind aber seit einiger Zeit Programme auf dem Markt (im Internet), die durch „Probieren“ (z. B. durch Abgleiche mit einem speziellen elektronischen Wörterbuch) und Verwendung verschiedener mathematischer Methoden die verschlüsselten Paßworte oder vergleichbare PIN ermitteln können. Dies ist um so schwieriger, je länger das Paßwort und je vielfältiger die Zeichenfolge ist. Für das Ermitteln

eines einfachen Paßwortes sind nur wenige Sekunden erforderlich. Selbst bei der Verwendung von alphanumerischen vier- bis fünfstelligen Paßworten liegt die Ratezeit noch im Minutenbereich. Derartige Angriffe sind jedoch in der Regel nur denjenigen Personen möglich, die Zugriff auf die Datei mit den verschlüsselten Paßwörtern haben. Auf die diesbezügliche „Allmacht der Systemverwalter“ habe ich in meinem 15. TB (s. dort Nr. 30.7) hingewiesen und die unkontrollierte volle Zugriffsmöglichkeit des Systemverwalters als sehr problematisch eingeschätzt, insbesondere dann, wenn es sich um besonders schützenswerte personenbezogene Daten handelt, die einem besonderen Amtsgeheimnis oder – wie hier – dem Fernmeldegeheimnis unterliegen.

Ein anderes Problem ergibt sich für den Anrufer:

Der „normale“ Anrufbeantworter und seine Funktion sind inzwischen bekannt. Dies gilt jedoch (immer noch) keineswegs für die T-Net-Box und ihren vom Verfügungsbereich des Inhabers abgesetzten Speicherort. Ich halte deshalb auch den Hinweis an den Anrufer für geboten, daß seine Nachricht nicht auf einem „normalen Anrufbeantworter im Wohnzimmer des Anrufers“ aufgezeichnet wird, sondern in einem System (Rechner) der DTAG. Dies folgt auch aus der Vorschrift des § 3 Abs. 4 Satz 1 TDSV, wonach der Diensteanbieter die Beteiligten in angemessener Weise über die Erhebung, Verarbeitung und Nutzung personenbezogener Daten zu unterrichten hat.

10.3.9 Werbung an Telefonkunden – immer wieder Ärger!

Die zum 1. Januar 1998 erfolgte vollständige Liberalisierung des in der Vergangenheit von der Deutschen Post beherrschten Telekommunikationsmarktes hat nicht nur zu einer quantitativen Zunahme der TK-Unternehmen und -Diensteanbieter, sondern auch zu einem deutlich gestiegenen Wettbewerb um Marktanteile in der Telekommunikationsbranche geführt. Dabei geht es neben den unternehmerischen Aktivitäten zur Gewinnung neuer Kunden zunehmend auch um Strategien und Maßnahmen, einen einmal gewonnenen Kundenstamm auch in der Zukunft zu halten. Auf der Grundlage der vorhandenen Kundendaten – Name, Anschrift, aber auch weiterer Informationen – nutzen die TK-Unternehmen und -Diensteanbieter hierzu die vielfältigen Möglichkeiten der Werbung, der Kundenberatung sowie der Marktforschung.

Immer wieder erreichen mich daher Fragen von Kunden, welche ihrer Daten das TK-Unternehmen für welchen Zweck nutzen darf. TK-Unternehmen und -Diensteanbieter dürfen nach § 89 Abs. 7 TKG die Bestandsdaten ihrer Kunden für Zwecke der Werbung, Kundenberatung oder auch Marktforschung nutzen, soweit dies erforderlich ist und der Kunde hierzu seine Einwilligung erteilt hat.

Diese Vorschrift bezieht sich allerdings nur auf die Nutzung für eigene Zwecke, also z. B. Werbung für das eigene Unternehmen, wie etwa die Unterbreitung eines Angebots über eine günstigere Tarifierung. Kunden, deren Bestandsdaten bereits vor Inkrafttreten des TKG (August 1996) von einem Unternehmen erhoben waren, hat der Gesetzgeber gegen eine solche Datennutzung ein Widerspruchsrecht eingeräumt, über das diese nach Inkrafttreten des TKG in angemessener Weise zu informieren waren (§ 89 Abs. 7 Satz 3 TKG).

Für eine weitergehende Nutzung von Kundendaten, wie ihre Übermittlung an andere Unternehmen (z. B. im Rahmen des Adressenhandels), ist eine gesonderte Einwilligung des Kunden erforderlich (§ 3 Abs. 1 Satz 2 TDSV).

Sofern der Kunde der Verwendung seiner Daten für Zwecke der (Eigen–)Werbung des Unternehmens nicht zugestimmt bzw. widersprochen hat, ist erst recht die Weitergabe der Daten an Dritte zu Werbezwecken (Adressenhandel und -vermietung) unzulässig. Das TK-Unternehmen darf die Daten selbst dann an Dritte zu Werbezwecken nicht weitergeben, wenn der Kunde sie für die Veröffentlichung im Telefonbuch und/oder im Kundenverzeichnis freigegeben hat.

Aufgrund verschiedener Anfragen von TK-Kunden bezüglich der Zulässigkeit der Nutzung von Bestandsdaten für Zwecke der Werbung, Kundenberatung oder auch Marktforschung sah ich mich veranlaßt, einzelne TK-Unternehmen und -Diensteanbieter nochmals auf die geltende Rechtslage und die diesbezüglichen Kundenrechte hinzuweisen.

Andererseits ist es aber auch grundsätzlich jedem erlaubt, Daten aus „allgemein zugänglichen Quellen“ – hierzu gehört auch das Telefonbuch – zu entnehmen und (auch) für Werbezwecke zu verwenden (§ 28 Abs. 1 Nr. 3 BDSG). Dies sollte der Telefonkunde bedenken, wenn er einwilligt, mit vollständigen Daten ins Telefonbuch oder in elektronische Verzeichnisse eingetragen zu werden.

10.3.10 Nur steter Tropfen höhlt den Stein – oder warum immer wieder Unterlagen im Müll gefunden werden

Eine in Baden-Württemberg erscheinende Tageszeitung schrieb im Dezember 1997 unter der Überschrift „Infos aus dem Müllcontainer“, daß Unterlagen von Kunden eines großen TK-Unternehmens einem frei zugänglichen Entsorgungscontainer entnommen werden konnten.

Im Zuge meiner Recherchen stellte sich heraus, daß während des Umzugs der am Ort ansässigen Niederlassung des Unternehmens veraltete und nicht mehr benötigte Akten entsorgt werden sollten. Der zu diesem Zweck angeforderte Entsorgungscontainer – der den an ihn zu stellenden Anforderungen in jeder Hinsicht entsprach – wurde in einem öffentlich zugänglichen Durchgang aufgestellt. Dort stand er für eine gewisse Zeit unverschlossen und unbeaufsichtigt. Ein aufmerksamer Passant sorgte dann durch einen entsprechenden Hinweis dafür, daß der Container verschlossen und mit einer Kette gesichert wurde.

Den der Zeitung vorgelegten Unterlagen war gemein, daß die Anschlüsse unter den angegebenen Nummern

nicht mehr existierten. Dies ändert jedoch nichts an der Rechtslage, daß auch für abgelaufene Verträge datenschutzrechtliche Anforderungen gelten, wobei Telekommunikationsunterlagen besonders schützenswert sind.

Das Unternehmen hat auf meine Kritik angemessen reagiert und mich im weiteren Verlauf bei der Erarbeitung einer Rahmenregelung zur datenschutzgerechten Entsorgung von personenbezogenen Unterlagen beteiligt. Die Regelung wurde in das firmeninterne Datenschutz-Handbuch übernommen. Damit wird jeder Organisationseinheit des Unternehmens eine Anleitung gegeben, um entsprechende orts- und aufgabenspezifische Regelungen ausgestalten zu können.

In einem anderen Fall übersandte mir ein Bürger Kopien der Aufträge von Kunden eines großen Mobilfunkunternehmens, die er im Flur eines Hauses gefunden haben wollte, in welchem sich auch ein Laden, ein sog. Shop, des Unternehmens befand. Die näheren Umstände des Auffindens ließen sich zwar nicht mehr aufklären, festzustellen war jedoch, daß jedenfalls zum Zeitpunkt des Auffindens der Unterlagen im Bereich des Shops die erforderlichen Maßnahmen der Zugangskontrolle, Datenträgerkontrolle und/oder Transportkontrolle unzureichend getroffen waren (§ 9 BDSG sowie Nrn. 1, 2 bzw. 9 der Anlage hierzu).

Obwohl es sich um gravierende Mängel handelte, die gemäß § 25 Abs. 1 BDSG zu beanstanden gewesen wären, habe ich zunächst von einer Beanstandung abgesehen, da ich der Stellungnahme des Mobilfunkunternehmens entnehmen konnte, daß zwischenzeitlich Maßnahmen ergriffen worden waren, um die Wiederholung solcher und ähnlicher Vorfälle – in allen Shops – künftig auszuschließen.

Auch hier zeigt sich:

Ausgefeilte Regelungen und anlaßbezogene Maßnahmen sind nur dann hilfreich, wenn sie Eingang in die Köpfe der Menschen finden, die sie umzusetzen haben. Nur die ständige Sensibilisierung für die Belange des Datenschutzes kann dauerhaft dazu führen, daß Datenschutz bewußt praktiziert wird.

11 Bundeskriminalamt

11.1 Das neue Bundeskriminalamtgesetz

Das neue Bundeskriminalamtgesetz – BKAG – vom 7. Juli 1997 trat am 1. August 1997 in Kraft. Damit wurden endlich die Vorgaben des Volkszählungs-Urteils umgesetzt und ein für die Informationsverarbeitung des BKA schwieriger rechtlicher Schwebezustand – nicht zuletzt vor den Verwaltungsgerichten – beendet. Für die Umsetzung des Gesetzes besteht jedoch weiterer Handlungsbedarf, woran ich das BMI frühzeitig erinnert habe. Dazu zählt in erster Linie der Erlaß einer Rechtsverordnung nach § 7 Abs. 6 BKAG, in der das BMI mit Zustimmung des Bundesrates das Nähere über die Art der Daten zu bestimmen hat, die nach den §§ 8 und 9 BKAG gespeichert werden dürfen. Diese Verordnung wird u. a. im Hinblick auf die Unterrichtungspflicht der Landeskriminalämter gegenüber dem BKA in dessen Funktion als Zentralstelle benötigt. Bisher ist das BMI seiner Verpflichtung nach § 7 Abs. 6 BKAG leider nicht nachgekommen. Dies ist mir unverständlich, weil die Regelungen des BKAG zum Teil nur einen Rahmen bilden, der weiterer Präzisierung bedarf.

Im übrigen bedürfen fast alle Errichtungsanordnungen, die das verbindliche Gerüst für automatisierte Dateien beim BKA bilden, nach § 34 BKAG der Anpassung an die gesetzlichen Regelungen und sind daher zu überarbeiten (zum Inhalt von Errichtungsanordnungen s. **Anlage 6**). Wie mir aus Gesprächen bekannt wurde, hat das BKA dem BMI überarbeitete Fassungen zugeleitet. Da formale Fragen noch nicht geklärt sind, bin ich bisher nicht beteiligt worden. Schließlich muß für das Verfahren der Protokollierung von Abrufen aus dem INPOL-System nach § 11 Abs. 6 BKAG ein schlüssiges Konzept gefunden werden, das für datenschutzrechtliche Kontrollen geeignet ist (vgl. auch Nr. 11.9).

Auch die Dateienrichtlinien und die KpS-Richtlinien sowie die Rahmenrichtlinien für den KAN, die aus den Jahren 1981 bzw. 1990 stammen, müssen an das novellierte BKAG angepaßt werden. Ich habe das BMI mehrfach auf diesen dringenden Handlungsbedarf zum BKAG hingewiesen; bisher kommt das BMI jedoch eher zögerlich seinen Verpflichtungen nach.

11.2 Rechtstatsachen

Bereits im 14. (Nr. 4.1.1) und im 15. TB (Nr. 1.10 und Nr. 11.2) habe ich eine wirksame Erfolgskontrolle bei strafprozessualen Eingriffsermächtigungen, wie z. B. der Telefonüberwachung nach § 100a StPO, gefordert. Nicht zuletzt mit Blick auf die im Zusammenhang mit der akustischen Wohnraumüberwachung eingeführten Berichtspflichten (vgl. Nr. 6.1) ist mir mehr denn je daran gelegen, diese Forderung auch für andere Ermächtigungen in die Praxis umzusetzen.

Wie angesprochen, hat der Gesetzgeber nunmehr für die Fälle der akustischen Wohnraumüberwachung sowohl der Staatsanwaltschaft gegenüber der obersten Justizbehörde (§ 100e Abs. 1 StPO) als auch der Bundesregierung gegenüber dem Bundestag Berichtspflichten auferlegt (§ 100e Abs. 2 StPO). Die Staatsanwaltschaft wird durch § 100e Abs. 1 StPO verpflichtet, der obersten Justizbehörde spätestens drei Monate nach Beendigung einer akustischen Wohnraumüberwachung über Anlaß, Umfang, Dauer, Ergebnis und Kosten der Maßnahme zu berichten. Ferner berichten die Staatsanwaltschaften, wann die Beteiligten nachträglich von der Maßnahme unterrichtet worden sind bzw. weshalb eine solche Benachrichtigung bislang unterblieben ist. Die Bundesregierung unterrichtet den Bundestag auf der Grundlage der Länderdaten jährlich über die durchgeführten Maßnahmen zur akustischen Wohnraumüberwachung (§ 100e Abs. 2 StPO). Damit wird für den Bereich der akustischen Wohnraumüberwachung rechtstatsächliches Material verfügbar, das für eine Erfolgskontrolle dieser tief in die Grundrechte eingreifenden Befugnis zwingend erforderlich ist.

Gleichartige Berichtspflichten sind unter anderem auch für den Bereich der Telefonüberwachung unabdingbar. Der aus Vertretern der Justizministerien von Bund und Ländern gebildete Strafrechtsausschuß „Statistiken und Berichte zum Einsatz technischer Mittel zum Abhören von Wohnungen und zu Telefonüberwachungen“ hat im Herbst 1998 seine Arbeitsergebnisse u. a. zum Bereich der Telefonüberwachung der Justizministerkonferenz vorgelegt, die diese Anfang November 1998 zur Kenntnis genommen hat. Nach deren Bericht hat die Arbeitsgruppe auf der Grundlage des TKG-Begleitgesetzes sowie des Gesetzes zur Verbesserung der Bekämpfung der organisierten Kriminalität die Erhebungsbögen für die Statistik zur Telefonüberwachung (Einzelerfassung und Zusammenfassung für die Behörden) sowie die Erläuterungen dazu überarbeitet und den Landesjustizverwaltungen zur Weiterleitung an die nachgeordneten Behörden übersandt. In dem Erhebungsbogen für die Fälle der Telefonüberwachung ist u. a. die Anzahl der Betroffenen, hinsichtlich derer im Berichtsjahr die Überwachung der Telekommunikation angeordnet wurde, aufzunehmen. Betroffene im Sinne des § 100a Satz 2 StPO sind danach Beschuldigte, Nachrichtenmittler oder ggf. Inhaber der vom Beschuldigten benutzten Telekommunikationsanschlüsse. Zudem sind die Verdachtstaten im Sinne des § 100a Satz 1 StPO zu bezeichnen. Der Erweiterung des Katalogs um die Tatbestände der Geldwäsche und der Verschleierung unrechtmäßig erlangter Vermögenswerte ist dabei Rechnung getragen worden. Die Bitte des Deutschen Bundestages vom 16. Januar 1998, Möglichkeiten einer einheitlichen statistischen Erfassung von Telefon- und Wohnraumüberwachungen zu prüfen und Vorschläge zur Verbesserung des Verfahrens der richterlichen Anordnung vorzulegen, konnte dagegen von der Arbeitsgruppe noch nicht vollständig erledigt werden, soll aber erneut aufgegriffen werden.

Die notwendige und von der Verfassung gebotene Erfolgskontrolle muß über besonders sensible strafprozessuale Ermittlungsmaßnahmen hinausgehen. Einzubeziehen sind auch präventiv-polizeiliche Befugnisse beispielsweise zur verdeckten Datenerhebung durch die Polizeien des Bundes und der Länder. Dabei dürfen Evaluation und Erfolgskontrolle methodisch nicht auf die Anlieferung und Auswertung statistischen Zahlenmaterials beschränkt werden. „Qualitative“ Erkenntnisse können sich auch aus der Befragung einer repräsentativen Auswahl von Anwendern polizeirechtlicher und strafprozessualer Eingriffsbefugnisse ergeben. Eine weitere wichtige, allein mit statistischen Mitteln jedoch nicht zu erfassende Variable dürfte die persönliche Einstellung von Richtern, Staatsanwälten und Kriminalbeamten zur Telefonüberwachung sein. Hier wäre u. a. zu klären, inwieweit die Telefonüberwachung nicht mehr als „ultima ratio“, sondern als bequeme Standardmaßnahme in jeder auch nur etwas komplexeren Ermittlung angesehen wird. Interessant wäre in diesem Zusammenhang, ob sich hier typische, mit zunehmender Distanz zur Ermittlung abgeschwächte, positive oder tendenziell kritische Grundeinstellungen ermitteln lassen, die für die Häufigkeit der Anwendung weitreichender Eingriffsbefugnisse ebenso entscheidend sein können wie die tatbestandlichen Voraussetzungen solcher Maßnahmen. Dabei ist eine intensive Beteiligung der Anwender, aber auch der Wissenschaft, unabdingbar.

Ich begrüße es daher ausdrücklich, wenn die Rechtstatsachensammelstelle beim BKA zur Verbreiterung ihrer Erkenntnisgrundlagen nicht nur Polizeipraktiker aus Bund und Ländern, sondern auch renommierte Kriminologen und meine Dienststelle beteiligt. Bei einer umfassenden, objektiven, kritischen und zugleich fairen Erfolgskontrolle kann es letztlich keine Gewinner und Verlierer geben, da sie auf das von allen Beteiligten gleichermaßen akzeptierte Ziel eines Freiheit und Sicherheit garantierenden Rechtsstaates gerichtet ist.

11.3 EUROPOL – Vertragsgesetz und Durchführungsbestimmungen, insbesondere Geschäftsordnung der Gemeinsamen Kontrollinstanz

Die Europäische Drogenstelle (EDS) als Vorläuferorganisation von EUROPOL hat im Berichtszeitraum den bi- bzw. multilateralen Informationsaustausch über die nationalen, nach Den Haag entsandten Verbindungsbeamten intensiviert, allerdings – mangels Rechtsgrundlage – weiterhin ohne eigenständige Verarbeitung personenbezogener Daten. Die EDS hat ferner in einzelnen Fällen die europaweite Koordinierung größerer Polizeiaktionen unterstützt, die zu zahlreichen Festnahmen geführt haben. Das Europäische Polizeiamt (EUROPOL) konnte trotz Inkrafttretens der Konvention zum 1. Oktober 1998 seine Arbeit noch nicht aufnehmen, weil die rechtlichen Voraussetzungen hierfür – neben der Ratifizierung des EUROPOL-Konvention vom 26. Juli 1995 durch die Mitgliedstaaten auch die Verabschiedung zahlreicher Durchführungsbestimmungen – noch nicht erfüllt waren. Unter anderem fehlte auch noch die Geschäftsordnung für die Gemeinsame Kontrollinstanz.

Das deutsche Vertragsgesetz vom 16. Dezember 1997 (BGBl. II S. 2150) regelt u. a. Fragen der Datenschutzkontrolle und der Haftung. Gemäß Artikel 2 § 6 Abs. 1 und 2 des EUROPOL-Gesetzes vertreten ein vom Bundesbeauftragten für den Datenschutz benannter Vertreter sowie ein vom Bundesrat benannter Vertreter der Landesbeauftragten für den Datenschutz die Belange des Datenschutzes in der **Gemeinsamen Kontrollinstanz**. Im Plenum der Gemeinsamen Kontrollinstanz wird Deutschland gegenwärtig durch mich persönlich und den LfD Sachsen-Anhalt vertreten, wobei ich das einheitliche, unteilbare Stimmrecht für die deutsche Delegation wahrnehme. Soweit Interessen der Länder berührt sind, habe ich nach Artikel 2 § 6 Abs. 2 Satz 3 des EUROPOL-Vertragsgesetzes die Stellungnahme des vom Bundesrat vorgeschlagenen Vertreters zu berücksichtigen. Während das Plenum der Gemeinsamen Kontrollinstanz zahlreiche Kontroll- und Beratungsfunktionen wahrzunehmen hat, hat der aus ihrer Mitte gebildete **Beschwerdeausschuß** nach Artikel 24 Abs. 7 der EUROPOL-Konvention eine aus deutscher Sicht eher gerichtsähn-

liche Funktion. Er überprüft insbesondere Beschwerden, die sich gegen die Verweigerung bzw. Teilverweigerung von Auskünften über die in den Analysedateien gespeicherten Daten richten. Mit Blick auf die verfassungsrechtlich gebotene Rechtsweggarantie ist im EUROPOL-Gesetz für den deutschen Vertreter die Befähigung zum Richteramt i.S. des deutschen Richtergesetzes als Berufungsvoraussetzung festgelegt worden. Die Unabhängigkeit des deutschen Vertreters im Beschwerdeausschuß wird u. a. durch eine ausdrückliche Regelung des Abberufungsverfahrens gesetzlich bekräftigt. Danach kann dieser – wie ein Richter – gegen seinen Willen nur durch Entscheidung eines Gerichtes aus dem Amt abberufen werden. Seine Mitgliedschaft ist also nicht an ein nationales Amt gebunden. Gegenwärtig bin ich der deutsche Vertreter im Beschwerdeausschuß.

Parallel zur Vorbereitung der nationalen Ratifizierungsverfahren berieten die Ratsgremien über zahlreiche Durchführungsbestimmungen zur EUROPOL-Konvention, wie z. B. das Personalstatut, die Haushaltsregelung, die Geheimschutzregelung, das Protokoll über Immunitäten und Privilegien der EUROPOL-Bediensteten, das Sitzstaatsabkommen mit dem Königreich der Niederlande, die Regelungen über den Informationsaustausch mit sog. Drittstaaten und Drittstellen sowie über die Durchführungsbestimmungen zu den Arbeitsdateien zu Analyse-
zwecken. Diese Rechtsakte sind vor Aufnahme der Tätigkeit von EUROPOL zu verabschieden.

Zum weiteren Kreis dieser Durchführungsbestimmungen kann auch die **Geschäftsordnung für die Gemeinsame Kontrollinstanz** gezählt werden, die das Verfahren dieses datenschutzrechtlichen Kontrollgremiums regelt. Entwürfe dieser Geschäftsordnung wurden von der Arbeitsgruppe „Polizei“ der europäischen Datenschutzbeauftragten vorbereitet. Ein erster Entwurf wurde im Oktober 1997 der Ratsarbeitsgruppe „EUROPOL“ vorgelegt. Nach Erörterung in dieser Ratsarbeitsgruppe und erneuter Diskussion und Ergänzung durch die Arbeitsgruppe „Polizei“ wurde der Entwurf von der im Oktober 1998 konstituierten Gemeinsamen Kontrollinstanz beschlossen. Im Rat konnte bisher kein Einvernehmen zu diesem Entwurf erzielt werden.

Sowohl in der AG „Polizei“ als auch in der Gemeinsamen Kontrollinstanz und den Ratsgremien wurden insbesondere die **Regelungen über das Verfahren vor dem Beschwerdeausschuß** sehr intensiv und teils kontrovers diskutiert. Mit Blick auf die gerichtsähnliche Funktion des Beschwerdeausschusses und die – auch bei Übertragung hoheitlicher Befugnisse auf EU-Institutionen zu beachtende – Rechtsschutzgarantie des Artikel 19 Abs. 4 GG, aber auch mit Blick auf Artikel 6 der Europäischen Menschenrechtskonvention wurde von den deutschen Vertretern in den beteiligten Gremien auf eine hinreichend gerichtsähnliche Ausgestaltung des Verfahrensablaufes, der Verfahrensrechte der Beteiligten und eine adäquate Sicherung der Unabhängigkeit und Qualifikation der Ausschußmitglieder hingewirkt. In intensiven und mitunter schwierigen Verhandlungen ist es gelungen, zentrale prozeßrechtliche Elemente, orientiert am deutschen Verfahrensrecht, einzubringen. Dies gilt z. B. für den Grundsatz der Öffentlichkeit der Verhandlung, aber auch für die Unabhängigkeit und Unparteilichkeit der Mitglieder des Ausschusses, den Ausschluß wegen Befangenheit, das Beweisantragsrecht des Beschwerdeführers, das Verbot des Austausches der zur Entscheidung berufenen Mitglieder des Ausschusses während des laufenden Verfahrens sowie für die Gewährung von Verfahrenskostenhilfe (Prozeßkostenhilfe). Allerdings bereitet das Prinzip der Öffentlichkeit des Verfahrens Frankreich noch große Schwierigkeiten, weshalb im Rat noch keine Einigung über die Geschäftsordnung erzielt werden konnte.

Regelungsumfang und -dichte der Geschäftsordnung des Beschwerdeausschusses sind geringer als im deutschen Prozeßrecht, was allerdings auch auf dessen sachlich begrenzten Aufgabenkreis zurückzuführen ist. Besonders wichtig und bemerkenswert erscheint mir die Befugnis des Beschwerdeausschusses zur umfassenden, unbeschränkten Kontrolle des entscheidungsrelevanten Sachverhalts.

Dabei hat der Beschwerdeausschuß sogar weitergehende Sachaufklärungsbefugnisse als z. B. ein deutsches Verwaltungsgericht, dem in den Fällen des § 99 Abs. 1 Satz 2 VwGO Informationen vorenthalten werden dürfen, wenn deren Bekanntwerden dem Wohl des Bundes oder eines deutschen Landes Nachteile bereiten würde oder wenn die prozeßrelevanten Vorgänge nach einem Gesetz oder ihrem Wesen nach geheim gehalten werden müssen. Dem deutschen Verwaltungsgericht ist in dieser Situation lediglich glaubhaft zu machen, daß die gesetzlichen Voraussetzungen für die Verweigerung der Vorlage von Urkunden oder Akten und die Erteilung von Auskünften vorliegen. Dies bedeutet jedoch nicht, daß dem Gericht zum Zwecke dieser Glaubhaftmachung stets der vollständige, geheimhaltungsbedürftige Sachverhalt offenzulegen ist. Demgegenüber verpflichtet Artikel 20 Abs. 2 der Geschäftsordnung EUROPOL, sozusagen alle Karten vollständig auf den Tisch zu legen, um dem Beschwerdeausschuß eine umfassende datenschutzrechtliche Prüfung zu ermöglichen. Zum Schutz besonders sensibler, geheimhaltungsbedürftiger Ermittlungen ist der Beschwerdeausschuß berechtigt, die Einsichtnahme des Beschwerdeführers und seines Vertreters in derartigen Fällen auszuschließen oder zu begrenzen. Auch mit dieser Verfahrensweise sind einige Mitgliedstaaten noch nicht einverstanden.

Angesichts der unterschiedlichen rechtlichen Traditionen und der darauf gegründeten Rechtssysteme der Mitgliedstaaten stellt die Geschäftsordnung der Gemeinsamen Kontrollinstanz zwangsläufig einen Kompromiß dar, der zeitnah auf seine Wirksamkeit hin überprüft werden sollte. Die Geschäftsordnung selbst sieht dies frühestens nach einem und spätestens drei Jahre nach ihrem Inkrafttreten durch die Beschwerdeausschuß vor. Insbesondere mit Blick auf die mittelfristig nach dem Amsterdamer Vertrag beabsichtigte Übertragung klassischer polizeilicher Ermittlungsbefugnisse auf EUROPOL wird sich die Frage erneut stellen, ob nicht besser ein Gericht die Maßnahmen dieser neuen europäischen Polizeibehörde überprüfen sollte.

11.4 Schengener Durchführungsübereinkommen

11.4.1 Überblick

Das Schengener Durchführungsübereinkommen (SDÜ) ist 1997 für Italien, Österreich und Griechenland stufenweise in Kraft gesetzt worden; dies bedeutet, daß Italien ab dem 26. Oktober, Österreich ab dem 1. Dezember und Griechenland ab dem 8. Dezember 1997 am Schengener Informationssystem (SIS) teilnehmen. Das SDÜ wird für diese Länder in mehreren Stufen in Kraft gesetzt, denn die Kontrollen an den Binnengrenzen wurden für Italien und Österreich erst im Frühjahr 1998 aufgehoben und sollen für Griechenland im Laufe des Jahres 1999 abgeschafft werden. Damit nehmen nunmehr 10 Mitgliedstaaten am SIS teil. Dementsprechend stieg die Zahl der Ausschreibungen auf mehr als 8 Millionen an (Stand: 12/98); darunter befinden sich ca. 800 000 Personenausschreibungen und mehr als 400 000 „alias"-Ausschreibungen. Das SIS, das ursprünglich für 5 Länder konzipiert war, stößt so allmählich an seine Kapazitätsgrenzen. Deshalb soll im Hinblick auf den bereits beschlossenen Beitritt von Dänemark, Finnland und Schweden zum SDÜ und die ebenfalls beschlossene Kooperation mit Island und Norwegen (vgl. 16. TB Nr. 11.6.1) das bestehende SIS kapazitätsmäßig kurzfristig so erweitert werden, daß die neuen Beitrittsländer im Jahre 2000 integriert werden können (sog. SIS I plus). Darüber hinaus sind bereits Projektstudien über ein völlig neu konzipiertes SIS II gestartet worden, das dem letzten Stand der Informations- und Kommunikationstechnik entsprechen und bis spätestens zum Jahre 2004 betriebsbereit sein soll. Das aktuelle SIS basiert noch auf dem technischen Standard von Ende der 80er Jahre.

Aufgrund eines Protokolls zum Amsterdamer Vertrag wird die auf dem Schengener Übereinkommen von 1985 und dem SDÜ von 1990 beruhende Zusammenarbeit inhaltlich und organisatorisch in die Europäische Union eingegliedert, d. h. der gesamte Schengen-Besitzstand einschließlich der Gemeinsamen Kontrollinstanz (GK) und des SIS wird auf die Union überführt. Diese Überführung wirft schwierige rechtliche und institutionelle Fragen auf, die bei Redaktionsschluß noch nicht alle geklärt waren; das soll jedoch bis zum Inkrafttreten des Amsterdamer Vertrages im Frühjahr 1999 abgeschlossen sein. Die meisten Schengen-Gremien, wie z. B. der Exekutivausschuß, werden ihre eigenständige Funktion verlieren und in die Organisation des Rates integriert; hingegen soll die GK ihre unabhängige Funktion weiterhin wahrnehmen.

11.4.2 Gemeinsame Kontrollinstanz

Wegen der bevorstehenden Integration der skandinavischen Länder können die Vertreter der dortigen Datenschutzkontrollinstanzen auf einstimmigen Beschluß der GK als Beobachter ohne Stimmrecht an den Sitzungen des Gremiums teilnehmen. Nach Inkrafttreten des Beitrittsvertrages mit der jeweiligen Vertragspartei werden die skandinavischen Vertreter zu Vollmitgliedern der GK.

Die GK hat im April 1997 in Lissabon ihren ersten und im April 1998 in Brüssel ihren zweiten Tätigkeitsbericht der Öffentlichkeit vorgestellt. Beide Berichte können in meiner Dienststelle angefordert werden. Einer der Schwerpunkte des ersten Berichts ist eine Zusammenfassung des Kontrollbesuchs von Vertretern der GK im Oktober 1996 beim C. SIS in Straßburg (vgl. 16. TB Nr. 11.6.2). Das Kontrollteam hat außerdem die wesentlichen Feststellungen in einem sog. technischen Bericht festgehalten, der als vertrauliches Dokument der Zentralen Gruppe übermittelt wurde. Der Bericht enthält wichtige datenschutzrechtliche Forderungen und Empfehlungen, z. B. zur Entwicklung eines neuen Datenabgleichsverfahrens, das die vollständige Identität der Datenbestände des C.SIS und aller N.SIS gewährleistet. Die Empfehlungen wurden jedoch von der Zentralen Gruppe als weniger bedeutend oder als derzeit nicht lösbar angesehen. Man beruft sich dabei insbesondere auf das geplante SIS II, mit dem sich einige der aufgezeigten Schwachstellen in Zukunft beheben ließen. Diese Antwort der Zentralen Gruppe läßt jedoch viele Fragen offen. Auch ist nicht hinnehmbar, daß man die GK ein gutes Jahr auf eine solche Antwort warten ließ. Ferner kann es nicht angehen, daß die festgestellten Mängel erst mit Inbetriebnahme des SIS II – also in ferner Zukunft – beseitigt werden sollen. Hier offenbart sich ein grundlegender Mangel in der Zusammenarbeit zwischen den Schengen-Gremien und der GK. Letztere muß früher und umfassender in den Schengener Entscheidungsprozeß eingebunden werden, soweit es um datenschutzrechtliche Probleme geht. Dies gilt insbesondere für den Ausbau des aktuellen SIS zum SIS I plus und mehr noch für die Neukonzeption des SIS II.

Darüber hinaus hat die GK im Berichtszeitraum eine Reihe von datenschutzrechtlichen Empfehlungen – z. B. zur Protokollierung von Abrufen aus dem SIS – gegeben, die in ihren Tätigkeitsberichten veröffentlicht sind.

Im Spätherbst 1998 startete die GK eine Informationsoffensive, um die Betroffenen beim Grenzübergang über ihre Rechte nach dem SDÜ aufzuklären, insbesondere über ihr Recht auf Auskunft nach Artikel 109 SDÜ. Zu diesem Zweck wurden in Deutschland an den wichtigen Grenzübergängen zu Drittstaaten, zu denen auch Flughäfen zählen, Plakate in deutscher und englischer Sprache angebracht, und Informationsfaltblätter mit dem Logo der GK zur Mitnahme ausgelegt. Ähnlich wurde bei den anderen Vertragsparteien verfahren. Damit soll ein wichtiger Beitrag für mehr Transparenz und Bürgerservice im Rahmen des Schengener Durchführungsübereinkommens geleistet werden.

11.5 Bilaterale Abkommen (Schengen/Extra-Schengen)

Seit mehreren Jahren führt die Bundesregierung, unterstützt von Vertretern der Länder, Verhandlungen auf bilateraler Basis mit europäischen Nachbarstaaten innerhalb und außerhalb des Schengener Vertragsgebietes über eine verstärkte polizeiliche Zusammenarbeit. Im 16. Tätigkeitsbericht (Nr. 11.9) habe ich die wesentlichen Regelungen des 1996 mit niederländischen Regie-

rungsstellen abgeschlossenen sowie des seinerzeit noch nicht fertiggestellten Abkommens über die polizeiliche Zusammenarbeit mit der Schweiz dargestellt. Inzwischen wurden entsprechende Verträge mit weiteren Nachbarstaaten vorbereitet. So laufen u. a. Verhandlungen mit **Belgien** und **Dänemark** zum Ausbau der grenzüberschreitenden polizeilichen Zusammenarbeit auf der Grundlage des SDÜ.

Der Entwurf eines deutsch-belgischen Abkommens über die Zusammenarbeit der Polizeibehörden und Zollverwaltungen in den Grenzgebieten orientiert sich an den Regelungen des **deutsch-französischen** Polizeikooperationsabkommens vom 9. Oktober 1997 und dem **deutsch-niederländischen** Abkommen aus dem Jahre 1996. Auch die polizeiliche Zusammenarbeit mit **Belgien** soll durch eine Optimierung des Informationsaustausches, die Koordination polizeilicher Einsätze im Grenzgebiet, eine Kooperation im Bereich der Aus- und Fortbildung und den Austausch von Sende- und Empfangsanlagen zur Erleichterung grenzüberschreitender Kommunikation verbessert werden. Der Entwurf enthält u. a. Detailregelungen der bereits im SDÜ vorgesehenen grenzüberschreitenden Observation und der dort ebenfalls geregelten grenzüberschreitenden Nacheile. Artikel 7 des Vertragsentwurfes läßt den Austausch von Erkenntnissen aus polizeilichen Informationssystemen und polizeilichen Unterlagen und dabei auch den Austausch polizeilicher Kenntnisse über Rauschgiftfälle durch die regionalen Verbindungsstellen im Grenzgebiet auf deutscher und belgischer Seite zu. Zu diesen Verbindungsstellen zählen auf deutscher Seite auch zwei Bundesgrenzschutzämter.

Der Vertragsentwurf mit **Dänemark** bewegt sich inhaltlich auf dem Niveau mit den zuvor erwähnten Schengen-Vertragsparteien; die Verhandlungen sind jedoch noch in einem frühen Stadium.

Ich gehe weiter davon aus, daß der **deutsch-schweizerische** Vertrag über polizeiliche Zusammenarbeit im Laufe des Jahres 1999 unterzeichnet werden kann. Da die Schweiz kein Mitglied des Schengen-Verbundes ist, sind die schweizerischen Polizeibehörden auch nicht an das Schengener Informationssystem (SIS) angeschlossen. Artikel 5 des deutsch-schweizerischen Polizeikooperationsvertrages soll diese wesentliche Informationslücke zumindest teilweise dadurch schließen, daß dem BKA und dem schweizerischen Bundesamt für Polizeiwesen der Austausch von Personenfahndungsdaten erlaubt wird. Damit wird die Schweiz zwar nicht an das SIS angebunden. Da die Bundesrepublik aber nach wie vor für einen Großteil der Schengen-Fahndungsdaten im SIS verantwortlich ist und diese nationalen deutschen Fahndungsdaten aufgrund des Polizeikooperationsabkommens künftig auch der schweizerischen Polizei zur Verfügung stehen sollen, rückt die Schweiz damit de facto deutlich näher an den Schengen-Verbund heran (daher auch die Bezeichnung „Extra-Schengen“). Mit Blick auf den insbesondere auf die Bundesrepublik zielenden Migrationsdruck aus Südosteuropa (vor allem aus dem ehemaligen Jugoslawien) und dem vorderen Orient (z. B. Irak) und die geographische Lage der Schweiz als Transitland auch für unerlaubte Einreisen in die Bundesrepublik Deutschland ist auch aus meiner Sicht vertretbar, Ausschreibungen deutscher Stellen zur Einreiseverweigerung, die nach Artikel 96 des SDÜ in das SIS eingestellt werden, der Schweiz auch automatisiert zu übermitteln. Angesichts des hohen datenschutzrechtlichen Niveaus in der Schweiz habe ich gegen die aus polizeilicher und asyl- bzw. ausländerrechtlicher Sicht im Abkommensentwurf vorgesehenen Befugnisse zur Datenübermittlung (u. a. auch Austausch von Fahrzeug- und Halterdaten) keine grundsätzlichen Bedenken. Eine abschließende datenschutzrechtliche Bewertung ist allerdings im Hinblick auf den Stand der Vertragsverhandlungen noch nicht möglich. Sie hängt letzten Endes von der Ausgestaltung der sog. Datenschutzklausel ab (vgl. 16. TB Nr. 11.9).

Die polizeiliche Zusammenarbeit mit den osteuropäischen Staaten steckt nach wie vor in dem Dilemma stark anwachsender, internationaler Kriminalität und meist fehlender – allenfalls rudimentärer – Datenschutzregelungen in diesen Ländern. Bereits im 16. TB habe ich darauf hingewiesen, daß eine möglichst kurzfristige Angleichung des datenschutzrechtlichen Niveaus, insbesondere auch der Datensicherheit, essentielle Voraussetzung eines polizeilichen Informationsaustausches ist, der über eine datenschutzrechtlich neutrale Übermittlung strategischer Lagebilder ohne personenbezogene Daten hinausgehend, auch detaillierte Informationen über beschuldigte und verdächtige Personen oder gar Opfer und Zeugen erfaßt. Dabei haben die Polizeibehörden im Inland in jedem Einzelfall sorgfältig zu prüfen, ob die angeforderten Informationen übermittelt werden dürfen, und dabei zu berücksichtigen, daß eine unkritische Übermittlung „weicher“ Daten und Erkenntnisse zu schweren Nachteilen für den möglicherweise unschuldigen Betroffenen, und – bei unzureichender Datensicherheit – auch für Zeugen und Opfer führen kann.

11.6 BKA im Internet

Kaum ein anderes Thema hat die Öffentlichkeit in den vergangenen Jahren so sehr bewegt wie die Entführung von Kindern und Jugendlichen, ihr Mißbrauch für pornographische Zwecke oder gar ihre anschließende Ermordung. Das Internet schafft Tatgelegenheiten für die Kommerzialisierung menschenverachtender sexueller Gewalt gegen Kinder, Jugendliche und Frauen. Anbieter und Abnehmer verfügen z. B. mit den Chat-Foren und News Groups über anonyme „Kontakthöfe“, auf denen weltweit und häufig mit recht geringem Entdeckungsrisiko einschlägige Darstellungen angeboten und Handelskontakte geknüpft werden können. Wie sehr die so erleichterte Verfügbarkeit von Pornographie und Gewaltdarstellungen die Nachfrage und damit letztlich auch das Risiko, Opfer zu werden, insbesondere für Kinder, Jugendliche und Frauen steigert, ist von den Strafverfolgungsorganen und der kriminologischen Forschung noch nicht abschließend geklärt. Die Gefahr einer Ausweitung strafrechtlich relevanter Pornographie und Gewaltdarstellung ist indes nicht von der Hand zu weisen. Der Ruf nach der „Polizeistreife im Internet“ ist deshalb allzu verständlich, zumal das Internet auch zur Begehung

weiterer Straftaten mißbraucht wird. Eine Umfrage des Rates bei den EU-Mitgliedstaaten ergab Fälle des Drogenhandels, der Propaganda für links- und rechtsextremistische Gruppen, der Wirtschaftsspionage, des Betruges, der Verletzung von Urheberrechten, der Bedrohung, Verleumdung und Beleidigung. Dabei sollte jedoch nicht außer Betracht bleiben, daß sich die weit überwiegende Mehrzahl der Internet-Nutzer gesetzeskonform verhält und deshalb nicht mit ungesetzlichen oder unverhältnismäßigen Ermittlungsmaßnahmen belastet werden darf.

Die datenschutzrechtliche Diskussion hierzu konzentriert sich auf folgende wesentliche Punkte:

Gesetzlich zu regeln war u. a. die strafrechtliche Verantwortlichkeit der Diensteanbieter, der Provider, die als natürliche oder juristische Personen oder Personenvereinigungen eigene Inhalte ins Internet einstellen oder fremden Inhalten den Weg ins Internet eröffnen (§ 5 Abs. 1 und 2 TDG). Danach sind Diensteanbieter für eigene Inhalte, die sie zur Nutzung bereit halten, nach den allgemeinen Gesetzen – d. h. auch nach Maßgabe des Strafgesetzbuches – verantwortlich. Das Bereithalten fremder Inhalte durch sog. Zugangs- oder Accessprovider i.S.d. § 5 Abs. 2 TDG führt dagegen nur dann zu strafrechtlicher Zurechnung, wenn die Zugangsprovider von den kriminellen Inhalten Kenntnis hatten und es ihnen technisch möglich und zumutbar war, deren Nutzung (Übermittlung) zu verhindern. Diese Regelung ist angemessen, sie verhindert kriminelle Angebote im Internet aber nicht (s. auch Nr. 8.1).

Deshalb stellt sich die Frage, in welchen Zonen des Internet die Polizei offen oder verdeckt zu präventiven, aber auch zu repressiven Zwecken ermitteln will. In diesem Zusammenhang ist zu klären, welche gesetzlichen Ermächtigungsgrundlagen für die Gewinnung von Erkenntnissen zu präventiven, aber auch zu Zwecken der Strafverfolgung erforderlich und angemessen sind. Während die Kenntnisnahme von offen und unbeschränkt für jedermann im Internet angebotenen Informationen durch die Polizei bereits durch die gesetzlichen Aufgabenzuweisungen des Polizeirechts bzw. der Strafprozeßordnung gedeckt wird, bedürfen Ermittlungseingriffe, wie z. B. eine getarnte Beteiligung an verdächtigen einschlägigen Chat-Foren durch verdeckte Ermittler, einer ausdrücklichen gesetzlichen Ermächtigung, da hier der staatliche Ermittler dem Verdächtigen bzw. dem polizeirechtlich relevanten Störer nicht offen erkennbar gegenübertritt. Dabei stellt sich die Frage, ob derartige Eingriffe anlaßunabhängig oder verdachtsunabhängig zugelassen werden dürfen, oder ob sie nur aufgrund eines hinreichend konkreten Verdachts oder einer hinreichend substantiierten Gefahr zugelassen werden sollten. Ein wahlloses Beobachten durch die Polizei von nicht allgemein zugänglicher und für Dritte unschädlicher privater Kommunikation würde letztlich zu einem Einschüchterungseffekt führen, der Meinungsfreiheit, Meinungsvielfalt und damit auch die Demokratie gefährden könnte.

Ein weiterer, auch datenschutzrechtlich relevanter Kernpunkt der Diskussion betrifft die Organisation und Koordination von Ermittlungen im Internet. Der Arbeitskreis II „Innere Sicherheit“ der Innenministerkonferenz hat sich Ende Oktober 1998 dafür ausgesprochen, anlaßunabhängige Recherchen im Internet durch das BKA als zentrale Stelle für das gesamte Bundesgebiet durchzuführen. Die Innenministerkonferenz hat sich dieser Empfehlung des AK II im November 1998 angeschlossen und darüber hinaus das BKA gebeten, ihr zur Herbstsitzung 1999 einen Erfahrungsbericht vorzulegen.

Das BSI wurde vom BMI beauftragt, eine sog. Meta-Suchmaschine zu entwickeln (vgl. Nr. 8.4), die die offenen Internet-Seiten nach kriminellen, strafrechtlich relevanten Inhalten durchsucht.

11.7 Geldwäsche

Im unmittelbaren Zusammenhang mit der Einführung der akustischen Wohnraumüberwachung (vgl. Nr. 6.1) soll durch das Gesetz zur Verbesserung der Bekämpfung der organisierten Kriminalität vom 4. Mai 1998 (vgl. Nr. 6.1.2) auch die Bekämpfung der Geldwäsche effektiver gestaltet werden. Deshalb wurden nicht nur der Geldwäschetatbestand im Strafgesetzbuch, sondern auch die Strafprozeßordnung, das Finanzverwaltungsgesetz und schließlich auch das Geldwäschegesetz geändert.

Wegen Geldwäsche kann nach der Änderung des § 261 Abs. 1 StGB durch Artikel 1 des Gesetzes zur Verbesserung der Bekämpfung der organisierten Kriminalität nunmehr auch der sog. Selbstwäscher bestraft werden, der selbst ein Verbrechen oder eines der in dieser Strafnorm benannten Vergehen begangen und dadurch Geld oder sonstige Vermögenswerte erlangt hat. Der Katalog der einschlägigen Vortaten einer Geldwäsche nach § 261 StGB wurde um zahlreiche Tatbestände erweitert.

Nach Änderung der Strafprozeßordnung durch Artikel 2 des vorgenannten Gesetzes sind nunmehr zur Aufklärung bei Verdacht der Geldwäsche sowohl die Telefonüberwachung (§ 100a Abs. 1 Nr. 2 StPO) als auch die akustische Wohnraumüberwachung (§ 100c Abs. 1 Nr. 3 Buchstabe a StPO) zulässig. Wegen der nicht unerheblichen Erweiterung des Vortatenkataloges zum Geldwäschetatbestand werden damit Telefonüberwachung und akustische Wohnraumüberwachung in zahlreichen Fallkonstellationen zulässig. Sowohl die Telefon- als auch die akustische Wohnraumüberwachung greifen tief in das Persönlichkeitsrecht der am Kommunikationsvorgang Beteiligten ein. Ich hoffe, daß die anordnenden Verantwortlichen, der Einzelrichter bei der Telefonüberwachung oder die Richter der zuständigen Kammer des Landgerichts bei der akustischen Wohnraumüberwachung, darauf hinwirken, daß diese sehr weitreichenden Eingriffsermächtigungen, die zwangsläufig auch Nichtverdächtige treffen, nur in sehr engen Grenzen in Anspruch genommen werden (zur Erfolgskontrolle strafprozessualer und anderer Eingriffsermächtigungen s. o. Nr. 11.2).

Mit dem Gesetz zur Verbesserung der Bekämpfung der organisierten Kriminalität wurde auch das Finanzverwaltungsgesetz novelliert, um die grenzüberschreitende Geldwäsche zu verhindern. So sind bei Grenzübertritt mitgeführtes Bargeld und gleichgestellte Zahlungsmittel im Wert von mindestens 30 000 DM auf Anfrage des

Zolls zu deklarieren. Dabei sind auch die Herkunft, der wirtschaftlich Berechtigte und der Verwendungszweck darzulegen (§ 12a Abs. 2 Satz 1 Finanzverwaltungsgesetz). Besteht Grund zur Annahme einer Geldwäsche, ist der Zoll berechtigt, das Bargeld oder die gleichgestellten Zahlungsmittel kurzfristig sicherzustellen (§ 12a Abs. 3 Satz 1 Finanzverwaltungsgesetz); ein nicht unerheblicher Eingriff in Freiheitsrechte von Bürgern, die die Grenze überschreiten.

Artikel 3 des Gesetzes zur Verbesserung der Bekämpfung der organisierten Kriminalität führte zu etlichen Änderungen des Geldwäschegesetzes. Aus meiner Sicht ist insbesondere auf die Neufassung des § 10 Abs. 2 GwG hinzuweisen. Während nach der bisherigen Regelung erst nach Abschluß der strafrechtlichen Ermittlungen geldwäscherelevante Tatsachen den Finanzbehörden mitgeteilt werden durften, ist dies nunmehr bereits unmittelbar nach Einleitung des Strafverfahrens zwingend vorgesehen (§ 10 Abs. 2 Satz 1 GwG). Die frühzeitige Unterrichtung der Steuerfahndung und der Finanzämter soll den raschen und rechtzeitigen fiskalischen Zugriff auf rechtswidrig erworbene Vermögenswerte sicherstellen. Die Anhebung des Schwellenwertes bei Bartransaktionen von bisher 20 000 DM auf 30 000 DM (§ 2 Abs. 1 und 2 sowie § 3 Abs. 1 Satz 1 GwG), wonach Betroffene zu identifizieren sind, hat dazu geführt, daß zahlreiche Datenerhebungen zur Person und zur jeweiligen Transaktion weggefallen sind, die sich nach altem Recht als überflüssig erwiesen hatten.

Auch die Polizeien von Bund und Ländern versuchen, die Bekämpfung der Geldwäsche effektiver zu gestalten. Zu diesem Zweck soll beim BKA eine sog. Verbunddatei zur bundesweiten Erfassung von Geldwäscheverdachtsfällen eingerichtet werden. Diese Datei soll sowohl vom BKA als auch von den Polizeibehörden der Länder genutzt werden. Als rechtlicher Rahmen für den Umfang der Datenspeicherung kommt § 8 BKAG in Betracht. Der erste Vorentwurf einer Errichtungsanordnung wurde mir im November 1998 übersandt (zum Inhalt einer Errichtungsanordnung s. **Anlage 6**). Mir ist besonders daran gelegen, daß nur solche Verdachtsfälle gespeichert werden, die zu staatsanwaltschaftlichen Ermittlungen geführt haben. Ferner sollten sog. Restverdachtsfälle (§ 8 Abs. 3 BKAG) nur dann und so lange gespeichert bleiben dürfen, als hinreichend gewichtige und abgesicherte Erkenntnisse für eine Verwicklung des Betroffenen in Geldwäscheaktivitäten sprechen. Von seiten des BMI und des BKA wurde weiter gefordert, sog. Transaktionsdaten, z. B. die Kontonummer des Zahlungsempfängers, ebenfalls zu erfassen. Dies setzt jedoch datenschutzrechtlich voraus, daß die betroffenen Personen zumindest als Kontaktpersonen i.S. von § 8 Abs. 4 BKAG anzusehen sind. Die Beratungen über den Entwurf der Errichtungsanordnung dauerten bei Redaktionsschluß noch an.

11.8 Automatisiertes Fingerabdruck-Identifizierungssystem – AFIS –

Bereits in meinem 15. Tätigkeitsbericht (Nr. 23.3) und in meinem 16. Tätigkeitsbericht (Nr. 11.4) habe ich über die Ergebnisse und deren Folgen einer im Jahre 1994 durchgeführten Kontrolle von AFIS berichtet. Im Verlauf dieser Kontrolle war auch deutlich geworden, daß die seinerzeit erstellte Errichtungsanordnung für AFIS nicht den gesetzlichen Anforderungen entspricht, weshalb ich stets auf eine Änderung gedrängt habe. Nach Inkrafttreten des BKA-Gesetzes im Jahre 1997 wird diese Forderung immer dringlicher. Denn § 34 dieses Gesetzes schreibt vor, daß das BKA für jede bei ihm zur Erfüllung seiner Aufgaben geführte automatisierte Datei mit personenbezogenen Daten eine Errichtungsanordnung nach bestimmten vorgegebenen Kriterien zu erstellen hat (s. hierzu **Anlage 6**). Trotz mehrfacher Erinnerung meinerseits liegt bisher keine diesen Anforderungen entsprechende Errichtungsanordnung vor. Ich habe dies gegenüber dem BMI **beanstandet**. Das BMI hat mir lediglich im Dezember 1997 mitgeteilt, es habe das BKA angewiesen, zwei Errichtungsanordnungen zu erstellen und zwar für AFIS-Fahndung und AFIS-Asyl. Ein Entwurf dieser Errichtungsanordnungen lag mir bei Redaktionsschluß noch nicht vor. Damit wird AFIS auch fünf Jahre nach seiner Inbetriebnahme weiterhin ohne ausreichende Rechtsgrundlage betrieben.

11.9 INPOL-Neukonzeption

In meinem 15. und 16. TB (Nr. 23.5; Nr. 11.3) habe ich über den jeweiligen Stand der konzeptionellen Arbeiten der Projektgruppe INPOL-neu beim BKA berichtet. In den letzten Jahren sind die Arbeiten an dem Konzept in eine entscheidende Phase getreten. Schließlich soll das neue Datenbanksystem bereits im Jahre 2000 das geltende INPOL-System ablösen. Die Datenschutzbeauftragten des Bundes und der Länder sind über eine eigene Arbeitsgruppe beteiligt, die auch über laufende Teilprojekte informiert wird. Daneben nehmen Vertreter der Datenschutzbeauftragten auch an Sitzungen der Projektgruppe teil. In periodischen Abständen, etwa zweimal im Jahr, findet ein Meinungsaustausch mit Vertretern des BMI, der Projektgruppe INPOL-neu beim BKA und den Vertretern der Arbeitsgruppe INPOL-neu der Datenschutzbeauftragten statt.

Da es sich bei dem neu zu konzipierenden Informationssystem um eine Verbund-Anwendung handelt, ergeben sich bereits aufgrund der unterschiedlichen Polizeigesetze in Bund und Ländern Probleme, die in dem Konzept für INPOL-neu gelöst werden müssen. Die Arbeitsgruppe der Datenschutzbeauftragten des Bundes und der Länder hat die nachfolgenden Schwerpunkte gesetzt und hierzu Papiere erstellt:

– Protokollierung

Nach § 11 Abs. 6 BKAG müssen Abrufe beim BKA protokolliert werden. Die Vorschrift hat folgenden Wortlaut:

> *„Werden beim BKA Daten abgerufen, hat es bei durchschnittlich jedem zehnten Abruf für Zwecke der Datenschutzkontrolle den Zeitpunkt, die Angaben, die die Feststellung der abgerufenen Datensätze ermöglichen, sowie die für den Abruf verantwortliche Dienststelle zu protokollieren. Die protokollierten Daten*

dürfen nur für Zwecke der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung eines ordnungsgemäßen Betriebes der Datenverarbeitungsanlage verwendet werden, es sei denn, es liegen Anhaltspunkte dafür vor, daß ohne ihre Verwendung die Verhinderung oder Verfolgung einer schwerwiegenden Straftat gegen Leib, Leben oder Freiheit einer Person aussichtslos oder wesentlich erschwert wäre. Die Protokolldaten sind nach zwölf Monaten zu löschen. Das BKA trifft die technischen und organisatorischen Maßnahmen nach § 9 des Bundesdatenschutzgesetzes.“

In der Projektgruppe bestanden zunächst unterschiedliche Meinungen, wie diese Rechtsnorm in der Praxis zu handhaben sei. Es wurde überlegt, ob die Protokollierung der wörtlichen Auslegung des Gesetzes folgend vorgenommen werden soll oder im Umfang der Begründung zum Gesetzesentwurf mit unterschiedlicher Behandlung von Einfach- und Mehrfachtreffern, oder ob sie ohne Differenzierung nach Mehrfach- und Einzeltreffern vorzunehmen sei. Im Verlauf der Diskussion verengte sich das Problem jedoch auf die Frage, in welchem Umfang Abfragen zu protokollieren sind. Das BMI vertritt die Auffassung, daß durchschnittlich zehn v. H. der Abfragen beim BKA zu protokollieren seien. Die Arbeitsgruppe der Datenschutzbeauftragten sieht § 11 Abs. 6 Satz 1 BKAG jedoch als Untergrenze der vom Gesetzgeber dem BKA auferlegten Protokollierungsverpflichtung an und empfiehlt, sämtliche Abrufe personenbezogener Daten vollständig zu protokollieren. Im übrigen wurde erneut auf die Zweckbestimmung für die Verwendung der Protokolldaten hingewiesen und angeregt, durch flankierende Maßnahmen den Risiken entgegenzuwirken, die durch eine im Gesetz vorgesehene Änderung der Zweckbestimmung bei der Nutzung der Protokolldaten für polizeiliche Belange entstehen können (s. auch **Anlage 23**).

– Speicherung von Daten nicht beschuldigter und nicht verdächtiger Personen

In der Projektgruppe INPOL-neu gab es in Anlehnung an die bisherige INPOL-Praxis Überlegungen, auch personenbezogene Daten von nicht beschuldigten und nicht verdächtigen Personen im Rahmen der INPOL-Neukonzeption zu speichern. Das können Daten von Personen sein, die z. B. im Zusammenhang mit der Beschlagnahme eines Notizbuches gefunden werden, die sich nicht auf die beschuldigte oder verdächtige Person beziehen, jedoch auch prima facie nicht eindeutig als irrelevant bewertet werden können.

Ich habe der Projektgruppe INPOL-neu nach Abstimmung mit den Vertretern der Arbeitsgruppe der Datenschutzbeauftragten mitgeteilt, daß § 8 Abs. 1 bis 5 BKAG den Personenkreis abschließend festlegt, der durch die Polizei in INPOL erfaßt werden darf. Die Speicherung anderer, dort nicht enumerativ aufgeführter Daten von Personengruppen scheidet daher aufgrund der bestehenden Gesetzeslage aus. Im übrigen bleiben landesrechtliche Vorschriften, insbesondere zur Speicherungsdauer und zum Zugriff auf bestimmte Datenarten unberührt.

– Datenverarbeitung für die Landeskriminalämter beim BKA

Bei einigen Ländern gibt es Überlegungen, ob in fest zu definierendem Umfang personenbezogene Daten, die nicht die Voraussetzungen des § 2 Abs. 1 BKAG erfüllen, quasi als Auftragsdatenverarbeitung auf dem Rechner im BKA für die Länder verarbeitet werden können. Für ein solches Vorhaben sprächen aus Sicht der Länder primär finanzielle Erwägungen. Obgleich ich diese fiskalischen Überlegungen nicht vollständig außer acht lassen kann, bin ich doch der Auffassung, die bestehende Rechtslage decke ein solches Projekt nicht ab. Aus meiner Sicht könnte lediglich § 2 Abs. 5 BKAG herangezogen werden, wonach das BKA die Länder auf Ersuchen bei deren Datenverarbeitung unterstützt. Danach erfolgen die Datenverarbeitung und Nutzung der Daten nach den Weisungen der Länder und nach deren Vorschriften über die Datenverarbeitung im Auftrag. Nach meiner Einschätzung läßt jedoch der Wortlaut der Gesetzesbegründung Auftragsdatenverarbeitung lediglich in besonderen Ausnahmefällen zu; das ist hier m.E. nicht erkennbar. Aber auch landesrechtliche Vorschriften könnten gegen diese Form der Datenverarbeitung sprechen. Die Projektgruppe INPOL-neu beim BKA hat sich zu dieser rechtlichen Konstruktion bisher noch nicht abschließend geäußert.

– Inhalt der Datei „Kriminalaktennachweis“ (KAN) beim BKA

Das BKA hat als Zentralstelle für das polizeiliche Auskunfts- und Nachrichtenwesen und für die Kriminalpolizei nach § 2 Abs. 1 BKAG die Aufgabe, die Polizeien des Bundes und der Länder bei der Verhütung und Verfolgung von Straftaten mit länderübergreifender, internationaler oder erheblicher Bedeutung zu unterstützen. Zur Erfüllung dieser Aufgabe führt das BKA den sog. KAN. Es handelt sich hierbei um ein Aktenhinweissystem. Im Rahmen der Arbeiten zu INPOL-neu und in Auslegung der gesetzlichen Regelung des § 8 BKAG überlegt die Projektgruppe, welchen Datenumfang die Datei in Zukunft haben wird. Von einigen Polizeien ist der Wunsch geäußert worden, auch in Anbetracht ökonomischer Gesichtspunkte, eine einheitliche Bestandsführung von Datenbeständen der Länder und den KAN nach einheitlichen Kriterien zu führen. Hierzu wurden zwei Lösungsvorschläge erarbeitet, die die Notwendigkeit aus polizeifachlicher Sicht begründen. Erst die Gesamtsicht aller Aktivitäten einer Person erlaube die Einstufung der Daten entsprechend den Kriterien, die für den KAN gelten. Dies treffe insbesondere auf die Beurteilung einer *„überregionalen Handlungsweise“* zu. Das polizeiliche Informationssystem müsse die Voraussetzung dafür schaffen, damit eine sachgerechte, an den Erfordernissen des § 2 Abs. 1 BKAG ausgerichtete Bewertung vorgenommen werden kann. Im Ergebnis führen beide Lösungsvorschläge dazu, daß Daten zu Delikten, die nach geltendem Recht nicht in den KAN beim BKA eingestellt werden dürfen, künftig dort gespeichert werden, sobald jemand mit einem Delikt in Erscheinung getreten ist, das die Voraussetzungen für die Aufnahme in diese Datei erfüllt. Die Vorschläge

unterscheiden sich grundsätzlich dahingehend, daß im Vorschlag A die – noch – nicht INPOL-relevanten Fälle zunächst im jeweiligen Landessystem verbleiben, während im Vorschlag B sofort alle Fälle in das polizeiliche Informationssystem beim BKA eingestellt werden, wobei die – noch – nicht INPOL-relevanten Fälle zunächst nur einem eingeschränkten Nutzerkreis sichtbar sind.

Die Arbeitsgruppe INPOL-neu der Datenschutzbeauftragten des Bundes und der Länder hat hierzu zwei Positionspapiere erstellt (**Anlagen 24** und **25**).

11.10 Kontrollen

11.10.1 Kontrolle der Protokollierung der Abrufe im nationalen Teil des Schengener Informationssystems

Nach Artikel 103 des Schengener Durchführungsübereinkommens (SDÜ) hat jede Vertragspartei zu gewährleisten, daß durchschnittlich jede zehnte Übermittlung von personenbezogenen Daten durch die dateiführende Stelle im nationalen Teil des Schengener Informationssystems protokolliert wird, um die Zulässigkeit der Abrufe zu kontrollieren. Nationaler Teil des Schengener Informationssystems ist der sogenannte Parallel-Datenbestand, der beim BKA geführt wird. Das BKA nimmt als nationale Stelle die Aufgaben aus dem SDÜ wahr. Zur Protokollierung habe ich dort angeregt, abweichend von der bisher praktizierten Zufallsprotokollierung Abrufe abschnittsweise aufzuzeichnen, wobei unter Abschnitt beispielsweise ein bestimmter Zeitraum zu verstehen ist. Ich bin der Auffassung, daß hierdurch Mißbrauchsfälle besser aufgedeckt werden können als durch eine Protokollierung nach dem Zufallsprinzip. Das BKA ist meiner Anregung nachgekommen und hat in einem bestimmten Zeitraum alle Anfragen an das System aufgezeichnet. Diese Datensätze habe ich nach von mir vorgegebenen Kriterien untersucht. Ich habe dabei u. a. festgestellt, daß ein Grenzschutzamt unzulässig Personalien aus dem Schengener Informationssystem abfragte. Die von mir eingeschaltete Grenzschutzdirektion teilte mir hierzu mit, daß ein disziplinarisches Vorverfahren gegen einen Beamten eingeleitet worden sei, dem mißbräuchliche Nutzung von INPOL-Datenträgern vorgeworfen wurde. Die Vorermittlungen dauerten bei Redaktionsschluß noch an.

Ich habe weiterhin festgestellt, daß die vorgelegten Protokolldaten nur begrenzt geeignet sind, die von den Vertragsparteien im SDÜ vorgesehene Zulässigkeit der Abrufe überprüfen zu können. Dies scheitert in vielen Fällen daran, daß auf die Unterlagen nicht zugegriffen werden kann, aus denen der Grund für die Speicherung der Daten im SIS hervorgeht. Eine solche Überprüfung ist nur möglich, wenn das BKA Akten zu der abgefragten Person führt. Ich habe daraufhin angeregt, daß künftig die Protokolldaten um eine Kennzeichnung ergänzt werden, die den Abfragenden eindeutig identifiziert, so daß nicht nur die abfragende Stelle, sondern auch die tatsächlich abfragende Person aus dem Protokolldatenbestand kenntlich wird. Ferner sollte, soweit die abfragende Stelle über Akten zu der abgefragten Person verfügt, systemtechnisch, spätestens im Rahmen der Neukonzeption von INPOL, realisiert werden, daß auch das Aktenzeichen aus dem gefundenen Datensatz mitprotokolliert wird. Hierdurch entstünde keine Mehrbelastung der zum Abruf befugten Mitarbeiter. Es wäre auch entschieden besser möglich, die Zulässigkeit der Abrufe nach Artikel 103 SDÜ zu kontrollieren.

Über die Konsequenzen aus meiner Kontrolle besteht im wesentlichen Einvernehmen mit dem BKA. Insbesondere wurde zugesagt, daß die Abfragen des SIS künftig regelmäßig abschnittsweise protokolliert werden. Zu meiner Anregung, die Protokollierung um die Aktenfundstelle zu erweitern, akzeptiere ich, daß dies über das derzeitige INPOL-Verfahren nicht realisiert werden kann, weil hierzu ein enormer Programmieraufwand betrieben werden müßte. Zur Übernahme einer eindeutigen Kennung des Abfragenden ist mir aus Erörterungen zum Verfahren INPOL-neu bekannt, daß eine eindeutige Benutzerkennung zukünftig Bestandteil der Protokolldaten werden wird.

Außer mit dem BKA habe ich auch mit der Gemeinsamen Kontrollinstanz nach Artikel 115 SDÜ das Problem der Protokollierung der Abrufe nach Artikel 103 SDÜ erörtert. Die Vertreter der nationalen Kontrollinstanzen haben hierzu eine Empfehlung an den Exekutivausschuß abgegeben. Danach ist die Gemeinsame Kontrollinstanz der Auffassung, daß folgende Mindestanforderungen einer ordnungsgemäßen Protokollierung nach Artikel 103 SDÜ gegeben sein müssen:

„1. Es muß ein hinreichend repräsentativer Durchschnitt aller Abrufe aufgezeichnet werden, unabhängig davon, ob die zugrunde liegende Abfrage positiv oder negativ beantwortet wird. Das Mindesterfordernis einer 10 v. H. Protokollierung kann auch durch abschnittsweise Aufzeichnung erbracht werden.

2. Zu den wesentlichen Elementen einer angemessenen Protokollierung zählen:

a) Übermittelte biographische Daten des Betroffenen, über den abgefragt wird;

b) Bezeichnung des Datenendgerätes oder der abrufenden Stelle, wobei dafür Sorge zu tragen ist, daß jede beliebige Maßnahme, die der Identifizierung des Benutzers dienen kann, ergriffen wird;

- *Ort, Datum und Zeitpunkt der Abfrage;*
- *Grund der Abfrage, z. B. Angabe der Rechtsgrundlage der Ausschreibung.*

Darüber hinaus hat es die Gemeinsame Kontrollinstanz für wünschenswert gehalten, daß das Aktenzeichen oder die polizeiliche Tagebuchnummer zum Wiederauffinden der zugrunde liegenden Akte, soweit vorhanden, im Einzelfall im Protokolldatenbestand aufgeführt wird.“

Die Entschließung der Gemeinsamen Kontrollinstanz habe ich dem BMI zugeleitet. Ich gehe davon aus, daß im Rahmen der INPOL-neu-Konzeption (vgl. Nr. 11.9) eine angemessene sachgerechte Lösung, die dem Zweck der Protokollierung entspricht, gefunden wird.

11.10.2 Arbeitsdatei „PIOS – Organisierte Kriminalität"

Im BKA wird eine Verbunddatei betrieben, in der Informationen zur Aufklärung und/oder vorbeugenden Bekämpfung von Straftaten der organisierten Kriminalität gespeichert werden: „PIOS – Organisierte Kriminalität". Ich habe diese Datei im Berichtszeitraum, jedoch vor Inkrafttreten des neuen BKA-Gesetzes, kontrolliert. Positiv konnte ich gegenüber dem BMI feststellen, daß mit dem Inkrafttreten des Gesetzes die – bisher fehlenden – notwendigen gesetzlichen Grundlagen für die Erhebung und Verarbeitung der Daten unterschiedlich „tatnaher" und „tatferner" Personen geschaffen wurden. Die Kontrolle hat ergeben, daß in dieser Datei auch Daten von Personen erfaßt sind, die nur gespeichert werden, weil sie mit Mitgliedern krimineller Vereinigungen im Ausland verwandt sind. Dies habe ich bemängelt, da dieser Umstand allein nicht ausreicht, um diese Daten in der Arbeitsdatei zu speichern. Der Sachverhalt wäre erst dann anders zu bewerten, wenn das der ausländischen kriminellen Vereinigung angehörende Mitglied in Deutschland eine Straftat begeht und damit dann der hiesigen Strafverfolgung unterliegt. Das BKA hat in einer ersten Stellungnahme die Erforderlichkeit der Speicherung mit kriminologischem Erfahrungswissen zu Täterstrukturen und -verhalten in diesem Kriminalitätsbereich begründet und darauf hingewiesen, daß es zu einem erheblichen Informationsverlust führte, wenn Daten dieses Personenkreises nicht erfaßt werden dürften. Zudem sei die Auswertung ausländischer Informationen und Berichte für die Bekämpfung der organisierten Kriminalität unerläßlich.

Ich habe Verständnis für die Besorgnisse des BKA; es bleibt aber festzuhalten, daß es keine Rechtsgrundlage für die Speicheurng der Daten des vorgenannten Personenkreises in polizeilichen Dateien gibt. Um das Problem sachgerecht zu lösen, habe ich unter Aufrechterhaltung der bisher von mir vertretenen Rechtsauffassung dem BMI und dem BKA vorgeschlagen, diese Daten, soweit keine eigenen Erkenntnisse deutscher Strafverfolgungsbehörden vorliegen, befristet in der Datei zu speichern. Sofern sich im Laufe dieses Zeitraums eigene kriminalpolizeilich relevante Erkenntnisse zu den Personen ergäben, komme gegebenenfalls eine weitere Datenspeicherung in Betracht. Darüber hinaus müsse gewährleistet werden, daß bezüglich dieser Daten eine strenge Zweckbindung für deren Nutzung gefunden wird. Ich habe angeregt, die Datennutzung ausschließlich für die Verbrechensbekämpfung im Rahmen der Organisierten Kriminalität zuzulassen. Darüber hinaus habe ich gefordert, daß bei Übermittlung dieser Daten die Empfänger über die zweckbestimmte Verwendung der Daten und das voraussichtliche Aussonderungsprüfdatum zu unterrichten sind.

Ich hoffe, daß meine Anregungen letztendlich aufgenommen werden und die Errichtungsanordnung (s. auch **Anlage 6**) für diese Arbeitsdatei aufgrund des novellierten BKA-Gesetzes präzisiert und ergänzt wird, obwohl das BMI in einer ersten Meinungsäußerung vom Dezember 1998 noch keine Bereitschaft hierzu signalisiert hat.

12 Bundesgrenzschutz

12.1 Der BGS kann jetzt nahezu jeden, auch verdachtsunabhängig, kontrollieren

Kurz vor Ende der 13. Legislaturperiode hat der Deutsche Bundestag das Erste Gesetz zur Änderung des Bundesgrenzschutzgesetzes vom 25. August 1998 (BGBl. I S. 2486) verabschiedet, mit dem die Befugnisse des Bundesgrenzschutzes bei der Personenkontrolle nicht unbeträchtlich erweitert wurden. Der Bundesgrenzschutz ist nach der Novellierung berechtigt, in Zügen und auf dem Gebiet der Bahnanlagen der Eisenbahnen des Bundes sowie in Anlagen oder Einrichtungen von Verkehrsflughäfen mit grenzüberschreitendem Verkehr verdachts- und anlaßunabhängig Personen kurzfristig anzuhalten, zu befragen und mitgeführte Ausweispapiere oder Grenzübertrittspapiere zu prüfen, sowie mitgeführte Sachen in Augenschein zu nehmen (§ 22 Abs. 1a – neu – BGSG). Die „verdachtslose Kontrolle" in Zügen und auf dem Gebiet der Bahnanlagen der Bundeseisenbahnen setzt nach einer Ergänzung des ursprünglichen Gesetzesentwurfes allerdings voraus, daß aufgrund von Lageerkenntnissen oder grenzpolizeilicher Erfahrung anzunehmen ist, daß diese Züge bzw. Bahnanlagen zur unerlaubten Einreise genutzt werden.

Immerhin wurde mit diesem ergänzenden Tatbestandsmerkmal versucht, den Anwendungsbereich dieser – immer noch sehr weiten – Erhebungsnorm etwas enger zu fassen. Mit der Novellierung wurde auch die Befugnis zur Identitätsfeststellung (§ 23 BGSG) erweitert. Danach ist die Identitätsfeststellung im Grenzgebiet bis zu einer Tiefe von 30 km nicht nur wie bisher zur Verhinderung oder Unterbindung unerlaubter Einreise, sondern auch zur Verhütung von Straftaten i.S.d. § 12 Abs. 1 Nr. 1 bis 4 BGSG zulässig, ohne daß dabei Tatsachen die Annahme rechtfertigen müssen, daß Straftaten begangen werden sollen. Mit dieser Erweiterung der Befugnis zur Identitätsfeststellung korrespondiert die Ergänzung des § 44 BGSG, der den BGS im Grenzgebiet auch zur Durchsuchung von Sachen ermächtigt.

Die Novellierung des BGSG wurde in den Medien und im Parlament lebhaft und kontrovers diskutiert, zumal Gesetzesvorhaben mit ähnlicher Zielrichtung (sog. Schleierfahndung) bereits zuvor in vier Bundesländern verabschiedet worden waren. Mit der Novellierung wird jedenfalls in dem o.g. Teilbereich das polizeirechtliche Grundprinzip aufgegeben, wonach die Polizei grundsätzlich nur gegen Störer und gegen Verdächtige, also anlaßbezogen, vorgeht. Auch wenn es sich bei den Änderungen in der Regel nur um kurzfristige Kontrollmaßnahmen handelt, so sind sie doch ein weiterer Eingriff in die Freiheitsrechte des Bürgers. Meine schriftlich dargelegten Bedenken gegen den Gesetzentwurf wurden von einigen der am 15. Juni 1998 im Innenausschuß des Deutschen Bundestages angehörten Sachverständigen geteilt. Nach dem Menschenbild des Grundgesetzes dürfe die Polizei nicht jedermann als potentiellen Rechtsbrecher betrachten, sondern hat davon auszugehen, daß die Bürger sich an Recht und Gesetz halten. Diese Redlichkeitsvermutung sei ebenso wie die Unschuldsver-

mutung des Artikel 6 Abs. 2 der Europäischen Menschenrechtskonvention konstitutives Merkmal unserer Verfassung. Ferner wurde gerügt, daß die „bundesweite Jedermannkontrolle“ über die dem BGS durch das Grundgesetz zugewiesene Grenzsicherungsaufgabe hinausgehe und eine am falschen Ort, nämlich im Bundespolizeirecht geregelte, materiell strafverfahrensrechtliche Dauerfahndung darstelle.

Dieser Kritik wurde durch andere Sachverständige widersprochen. Grenzbezogene Sachverhalte seien von jeher Anknüpfungspunkte für verdachtsunabhängige Personenkontrollen gewesen. Die Identitätsfeststellung als solche führe lediglich zu einem vergleichweise geringfügigen Grundrechtseingriff, da die Kontrolle nur wenige Sekunden bis Minuten in Anspruch nehme. Mit Blick auf das verfassungsrechtliche Gebot der Verhältnismäßigkeit sei aber sicherzustellen, daß der Kontrollanlaß (Verhinderung bzw. Unterbindung unerlaubter Einreise, Verhütung von Straftaten) sich auf objektivierbare tatsächliche Anhaltspunkte stützen lasse. Für Durchsuchungsmaßnahmen bedürfe es weiterer tatsächlicher Anhaltspunkte, die einen derart intensiven, über die bloße Personalienfeststellung hinausgehenden Grundrechtseingriff rechtfertigen könnten.

Der Gesetzgeber ist dieser Anregung gefolgt und setzt für die Ausübung der Befugnisse nach § 22 Abs. 1a – neu – BGSG nunmehr voraus, daß aufgrund von Lageerkenntnissen und grenzpolizeilicher Erfahrung anzunehmen ist, daß die kontrollierten Züge oder Bahnanlagen zur unerlaubten Einreise genutzt werden. Mit Blick auf die verfassungsrechtliche Sensibilität der Novellierung begrüße ich es, daß der Deutsche Bundestag meine Anregung zur Befristung der erweiterten Befugnisse nach § 22 BGSG bis Ende des Jahres 2003 aufgegriffen und damit eine intensive Evaluation dieser – auf Bundesebene – neuartigen Eingriffsermächtigung ermöglicht hat.

12.2 Integrierte Vorgangsbearbeitung durch den BGS

Auch der BGS ist, wie das BKA und die Polizeien der Länder, Teilnehmer am polizeilichen Informationssystem INPOL, das gegenwärtig grundlegend umstrukturiert und optimiert wird (vgl. Nr. 11.9 – INPOL – neu –). Der BGS nutzt diese Umstellung, um die – auch arbeitsökonomisch gebotene – Modernisierung seiner polizeilich-operativen, automatisierten Datenverarbeitung durchzuführen. Zu diesem Zweck will der BGS Informationsflüsse beschleunigen und qualitativ verbessern, die bisher gewohnte Mehrfacherfassung polizeilich relevanter Daten vermeiden und wertvolle Arbeitszeit z. B. dadurch einsparen, daß Statistiken und Führungsinformationen automatisiert erstellt werden. Die Einführung der integrierten polizeilichen Vorgangsbearbeitung – IPV-BGS – stellt – nach der Neuregelung der Aufgaben (1992) und der Strukturen (1997/98) des BGS – eine der wichtigsten Reformen dieser zahlenmäßig größten Bundespolizei dar.

Kernpunkt der IPV-BGS ist die sog. Einmalerfassung von Personen- und Sachdaten sowie von Sachverhalten und deren durchgängige Speicherung. Schreibmaschine, Durchschlagpapier und Formularsätze auf dem Schreibtisch des BGS-Beamten werden überflüssig, wenn beispielsweise die Personalien von Schleusern und Geschleusten mit den Sachverhaltsdaten unmittelbar nach der Festnahme im PC der zuständigen Grenzschutzinspektion erfaßt und ohne Medienbruch, z. B. in Falldateien, und – anonymisiert – in regionale und bundesweite Statistiken, Lagebilder und andere Führungsinformationen übernommen werden können. Die Dateianwendung „elektronisches Tagebuch/ Vordrucke“ soll einen umfassenden, chronologischen Nachweis aller polizeilichen Aktivitäten, eine schnelle Lagebeurteilung und einen rationellen Einsatz der Beamten und der Führungs- und Arbeitsmittel ermöglichen.

Elektronische Tagebücher sollen bei jeder BGS-Dienststelle geführt werden. Auszugsweise können Daten des elektronischen Tagebuchs in ein überörtliches und überregionales Auswerte- und Recherchesystem überführt werden, aus dem – wiederum verdichtete und anonymisierte – Daten in eine strategische Auswertung zur Erstellung von Kriminalitätslagebildern und strategischen Ergebnisdateien übernommen werden können. Zugleich sollen damit Bekämpfungskonzeptionen und Fahndungsraster leichter möglich werden. Das System IPV-BGS wird aber auch mit Dateien zur operativen Auswertung (z. B. Falldateien, Telefonüberwachungsdateien und operative Ergebnisdateien) verknüpft sein.

Ich verkenne nicht, daß moderne, schnelle und effektive polizeiliche Informationssysteme notwendig sind. Die neuartige polizeiliche Datenverarbeitung muß aber transparent und überschaubar bleiben. Dies bedeutet u. a. eine klare und präzise Definition der Zugriffsmöglichkeiten der verschiedenen Nutzer auf den unterschiedlichen Hierarchieebenen des Systems, präzise Definition der in den verschiedenen Anwendungen zu speichernden Datenarten, Gewährleistung und nicht nur oberflächliche Durchführung der Prüfung weiterer Erforderlichkeit gespeicherter Daten und die fristgerechte Löschung nicht mehr erforderlicher Daten in allen Dateien. Ferner sind effektive Mechanismen zur Berichtigung fehlerhafter Datensätze zu schaffen. Authentizität, Richtigkeit und Erforderlichkeit der Daten sowie Maßnahmen zur Datensicherheit liegen aber nicht nur im Interesse des Datenschutzes, sondern auch im Interesse der Anwender.

Die Grenzschutzdirektion hat mich bei der Entwicklung der Konzeption frühzeitig, intensiv und umfassend beteiligt. Eine endgültige datenschutzrechtliche Beurteilung ist jedoch erst dann möglich, wenn mir die erforderlichen Errichtungsanordnungen (s. hierzu **Anlage 6**) für die Umsetzung der Konzeption vorliegen.

12.3 Telefaxe auf Abwegen

Wiederholt habe ich auf die Gefahren beim Telefaxverkehr hingewiesen und Vorschläge für eine sichere Nutzung dieses Kommunikationsmittels gemacht (16. TB Nr. 10.4.13 und Anlage 13 zum 13. TB). Trotzdem kommt es mitunter zu Fehlübermittlungen, wie das folgende Beispiel zeigt:

Über mehrere Monate liefen dienstliche Telefaxe, die für eine Grenzschutzstelle bestimmt waren, bei einem Düsseldorfer Bürger auf, der sich über die wiederholten Fehlübermittlungen beschwerte. Mehrere Telefaxe enthielten personenbezogene Daten und grenzpolizeiliche Informationen, die nicht für Dritte bestimmt waren.

Das BMI teilte mir mit, es sei nicht mehr feststellbar, ob es über die eindeutig belegten Fälle hinaus zu weiteren falsch zugeleiteten Telefaxen gekommen sei. Die auch vom BMI bestätigten Fehlleitungen wurden darauf zurückgeführt, daß nach einem Großbrand im Bereich der betroffenen Grenzschutzstelle im April 1996 zeitgleich unterschiedliche Telefon- und Telefaxgeräte genutzt werden mußten. An manchen Geräten mußte zunächst die „0“ eingegeben werden, während bei anderen Geräten diese Kennziffer bereits automatisch vorgewählt wurde, um in das öffentliche Telefonnetz zu gelangen. Die kombinierte Telefon- und Telefaxnummer des unfreiwilligen Empfängers gleicht – abgesehen von der „0“ am Anfang – den ersten sieben Ziffern der Telefaxnummer des richtigen Adressaten, einer anderen Grenzschutzstelle. Ursächlich für die Fehlleitungen war aber auch eine unzureichende Organisation der Telekommunikation bzw. eine unzureichende fachliche Aufsicht.

Die Leitung der BGS-Dienststelle hätte sich rechtzeitig um einheitliche und sichere, gegen Bedienungsfehler weitgehend unempfindliche Telefax-Verbindungen bemühen müssen. Die Installation von Telefaxgeräten mit Vorwahltasten und Adressatenspeicher wäre ein geeignetes Mittel gewesen, Fehlübermittlungen weitgehend auszuschließen. Jede Grenzschutzstelle hat nach § 9 BDSG sicherzustellen, daß Telefaxe so übermittelt werden, daß eine fehlerhafte Zuleitung aus Sicht der Dienststelle ausgeschlossen werden kann. Dieser Verpflichtung ist die betroffene Grenzschutzstelle über einen längeren Zeitraum nicht hinreichend nachgekommen. Ich sehe bereits in der Hinnahme dieses Risikos einen nicht unerheblichen Verstoß gegen die Verpflichtungen aus § 9 BDSG. Das Risiko erneuter Fehlübermittlungen ist nunmehr durch die Bereitstellung von Fax-Geräten mit Vorwahltasten stark reduziert. Die bundesweite Anwendung der vom BGS gemeinsam mit meiner Dienststelle entwickelten „Nutzungsbestimmungen für den Gebrauch von Faxgeräten“ dürfte darüber hinaus – nicht nur bei der betroffenen Dienststelle des BGS – das Risiko vergleichbarer Verstöße künftig weiter mindern. Aus diesem Grunde hielt ich es für vertretbar, gemäß § 25 Abs. 2, 2. Alternative BDSG von einer Beanstandung abzusehen.

12.4 Paßersatzbeschaffung

Vom sächsischen Ausländerbeauftragten wurde mir der Fall eines tunesischen Staatsangehörigen übermittelt, der im Jahre 1993 in Deutschland einen Asylantrag gestellt hatte. Zur Durchführung des Asylverfahrens hatte der Betroffene auch seinen Militärausweis bei der Aufnahmeeinrichtung für Asylbewerber abgegeben. Da der Betroffene wenige Jahre später eine deutsche Staatsangehörige heiratete, war das Asylverfahren damit beendet, und er begehrte nun die Herausgabe aller zur Durchführung des Asylverfahrens einbehaltenen Dokumente. Außer seinem Militärpaß erhielt er diese auch. Über den Verbleib dieses Dokuments konnte ihm die Behörde zunächst keine Auskunft geben. Nach mehrmonatigen intensiven Nachforschungen wurde ihm dann mitgeteilt, daß sein Militärpaß über die Grenzschutzdirektion Koblenz an das tunesische Generalkonsulat in Berlin gesandt worden sei und er sich den Paß dort abholen könne. Der Petent sah sich in einer sehr unangenehmen Lage, weil mit der Übersendung seines Militärpasses an eine Behörde seines Heimatlandes der Umstand seines Asylantrages offenbart wurde. Er war besorgt um die Sicherheit seiner Familie, die noch in Tunesien lebt.

Ich habe die Sache geprüft und bin zu dem Ergebnis gelangt, daß die Datenübermittlung nach § 32 Abs. 3 des BGSG unter den dort genannten Voraussetzungen zulässig ist. Nach § 33 Abs. 6 BGSG hätte jedoch der Datenempfänger, die tunesische Behörde, auf den beabsichtigten Löschungszeitpunkt und auf die Zweckbestimmung bei der Verwendung hingewiesen werden müssen. Diesen Verpflichtungen ist die Grenzschutzdirektion nicht nachgekommen. Im vorliegenden Fall ist das tunesische Generalkonsulat im nachhinein über die Zweckgebundenheit der übermittelten Daten und die durch die Beendigung des Asylverfahrens eingetretene Verpflichtung zur Löschung der Daten hingewiesen worden. Darüber hinaus hat die Grenzschutzdirektion zugesichert, daß künftig bei jeder Übermittlung personenbezogener Daten im Zuge der Beschaffung von Heimreisedokumenten mit einem Standardtext auf die Zweckbindungsregelung des § 33 Abs. 6 BGSG hingewiesen wird. Außerdem wird – ebenfalls als Ergebnis meiner Kontrolle – zukünftig stets der voraussichtliche Löschungstermin der gespeicherten personenbezogenen Daten der ausländischen Stelle mitgeteilt werden.

13 Zollfahndung

13.1 Noch immer keine bereichsspezifischen Datenschutzregelungen für das Zollkriminalamt und den Zollfahndungsdienst

Auch 15 Jahre nach Erlaß des Volkszählungs-Urteils steht eine bereichsspezifische und normenklare Rechtsgrundlage für das Zollkriminalamt (ZKA) und den gesamten Zollfahndungsdienst (vgl. 15. TB Nr. 25.1) immer noch aus. Hatte es von Seiten des verantwortlichen BMF früher immer geheißen, nach Inkrafttreten eines BKAG (vgl. Nr. 11.1) sei mit der baldigen Vorlage eines entsprechenden Gesetzentwurfs zu rechnen, so herrscht nun mehr oder weniger Funkstille in dieser leidigen Angelegenheit; und dies ungeachtet der Tatsache, daß auch der Deutsche Bundestag anläßlich der Billigung einer Beschlußempfehlung des Innenausschusses zu meinem 16. TB (Plenarprotokoll 13/244 über die Sitzung vom 24.06.1998) die Bundesregierung aufgefordert hat, alsbald einen solchen Gesetzentwurf einzubringen (s. **Anlage 4**). Ich habe größte Zweifel, ob sich das BMF noch weiter auf einen nach der Rechtsprechung des Bundesverfassungsgerichts grundsätzlich möglichen Übergangsbonus berufen kann. Denn die Notwendigkeit von

gesetzlichen Regelungen aufgrund gewandelter Verfassungsinterpretation (des Volkszählungs-Urteils) hat sich bereits vor 15 Jahren ergeben und die Bundesregierung kann sich nicht länger darauf zurückziehen, es gelte eine ansonsten eintretende Funktionsuntüchtigkeit staatlicher Einrichtungen zu vermeiden, die der verfassungsmäßigen Ordnung noch ferner läge als der bisherige Zustand. Jedenfalls müssen sich das ZKA und der Zollfahndungsdienst bis auf weiteres auf diejenigen Eingriffsmaßnahmen beschränken, die für ihre Funktionsfähigkeit unerläßlich sind. Dies gilt insbesondere für die Datenspeicherung im INZOLL-System (s. u. Nr. 13.2).

Ebenso ist die Rechtsverordnung nach § 5a Abs. 2 des Finanzverwaltungsgesetzes über die Übermittlung von Daten durch das ZKA (vgl. 16. TB Nr. 13.3), wozu mir bereits seit mehr als sechs Jahren ein Entwurf vorliegt, immer noch nicht verabschiedet. Hauptstreitpunkt dürfte hier die Aufnahme der Nachrichtendienste in den Kreis der Datenempfänger sein. Ungeachtet dieser Schwierigkeiten halte ich es für nicht akzeptabel, daß die Bundesregierung mehr als sechs Jahre nach Inkrafttreten des Gesetzes zur Änderung des Finanzverwaltungsgesetzes und anderer Gesetze ihren gesetzlichen Verpflichtungen noch immer nicht nachkommt.

13.2 INZOLL

In meinem 16. TB (Nr. 13.5) hatte ich einzelne Kritikpunkte an dem damaligen Entwurf einer Errichtungsanordnung für die Datei INZOLL aufgeführt. Nachdem ich im Berichtszeitraum mit Vertretern des BMF weitere Gespräche zu diesem Entwurf geführt habe, konnte zwar nicht in allen Punkten Einigung erzielt werden. Gleichwohl habe ich der nachgebesserten Fassung unter Aufrechterhaltung meiner bisher geäußerten Bedenken und vorbehaltlich der noch ausstehenden gesetzlichen Regelung (vgl. Nr. 13.1) zugestimmt. Zu den gesetzlichen Anforderungen an eine Errichtungsanordnung siehe **Anlage 6**.

In folgenden Punkten habe ich Verbesserungen erreichen können:

Der ursprünglich in der Errichtungsanordnung vorgesehene und in der Praxis bis dahin bestehende Zugriff des zuständigen Referates im BMF auf sämtliche Datensätze der Datei INZOLL ist aufgehoben worden. Die Errichtungsanordnung sieht in diesem Punkt nunmehr vor, daß die zuständigen Referate des BMF nur noch konventionell übermittelte personenbezogene Daten aus INZOLL im Einzelfall nutzen dürfen. Dies halte ich aus Gründen der dem BMF obliegenden Fachaufsicht über den Zollfahndungsdienst für sachgerecht.

Die neue Errichtungsanordnung sieht nicht mehr vor, daß Amtshilfeersuchen ausländischer Behörden gespeichert werden. Hiergegen hatte ich mich aufgrund von Kontrollergbnissen bei verschiedenen Zollfahndungsämtern und Zollfahndungszweigstellen gewandt. Bisher wurde es aufgrund der wachsenden Mobilität der Täter als erforderlich angesehen, Amtshilfeersuchen in INZOLL zu speichern. Diese Position hat das BMF aufgegeben, zumal das Verfahren auch daran krankte, daß grundsätzlich keine Rückmeldung der ersuchenden ausländischen Behörden über den Verfahrensausgang gegeben wurde, was dazu führte, daß die gespeicherten personenbezogenen Daten unterschiedslos lange (zehn Jahre) in INZOLL gespeichert blieben.

Ferner habe ich erreicht, daß die bisher gültige Regelung über die Speicherungsdauer der Datensätze differenzierter wurde. Nach der neuen Errichtungsanordnung sind abgestufte Speicherungsfristen zwischen sechs Monaten und zehn Jahren vorgesehen. Eine weitere Differenzierung wird bei festgesetzten Geldbußen anhand der Betragshöhe vorgenommen.

Auch die Prüffristen für die Aussonderung, d. h. die Löschung der Daten, werden jetzt datenschutzfreundlicher festgelegt. Während nach der alten Regelung der letzte Tag der Verarbeitung der personenbezogenen Daten die Frist für die Dauer der Aufbewahrung auslöste, ist nunmehr, wie es auch bei anderen Behörden der Praxis entspricht, grundsätzlich der Tag des Ereignisses, an das die Speicherung personenbezogener Daten anknüpft, für die Fristberechnung entscheidend. Darüber hinaus sind die Zollfahndungsstellen nun gehalten, bei jeder Einzelfallbearbeitung und nach den von ihnen festgesetzten Fristen (Aussonderungsprüffristen) die weitere Erforderlichkeit der Datenspeicherung zu überprüfen.

13.3 Kontrollen bei Zollfahndungsdienststellen

Im Berichtszeitraum habe ich wiederum eine Zollfahndungszweigstelle kontrolliert. Leider habe ich erneut Mängel festgestellt, die ich bereits bei früheren Kontrollen (vgl. 16. TB Nr. 13.6) bei anderen Zollfahndungsdienststellen vorgefunden hatte.

Darüber hinaus habe ich in den Aktenunterlagen der Zollfahnungszweigstelle Erfassungsbögen mit Ergebnissen von erkennungsdienstlichen Behandlungen festgestellt, die von Landespolizeidienststellen übermittelt worden waren. Nach meiner Auffassung gibt es keine rechtliche Grundlage für die Übermittlung und die Aufbewahrung dieser Unterlagen bei der Zollfahndungszweigstelle. Mit der geprüften Stelle bestand Einvernehmen, derartige Unterlagen künftig nicht mehr in den Ermittlungsakten der Zollfahndungszweigstelle zu führen.

In einem anderen Fall habe ich festgestellt, daß personenbezogene Daten von jemandem, der eine Person mit einer geringen Menge Haschisch in seinem Fahrzeug mitgenommen hatte, erfaßt und in einer Akte gespeichert worden sind. Darüber hinaus wurde auch eine Kopie des Kfz-Scheins zur Akte genommen. Dieser war ausgestellt auf den Namen einer am Vorfall unbeteiligten Person, also keiner der Fahrzeuginsassen. Auch hier konnte während der Kontrolle erreicht werden, Kopien von Unterlagen über nicht tatbeteiligte Personen spätestens bei Abschluß der Ermittlungen aus der Akte herauszunehmen und zu vernichten.

Problematisiert habe ich ferner, daß unverhältnismäßig lange Fristen für die Prüfung, ob Daten gelöscht werden können, in Bagatellfällen vergeben werden. Dies hatte

ich bereits aus früherem Anlaß gegenüber dem BMF gerügt. Das BMF hat in einer ersten Stellungnahme Zweifel an meiner Kontrollkompetenz geäußert. Diese Bedenken begründeten das BMF sowie das ebenfalls eingeschaltete ZKA nach Abstimmung mit den Generalstaatsanwaltschaften Düsseldorf und Köln damit, die Angehörigen des Zollfahndungsdienstes seien gemäß § 404 AO Hilfsbeamte der Staatsanwaltschaft und unterlägen somit der Sachleitungsbefugnis der Staatsanwaltschaft. Folglich könnten die Zollfahndungsdienststellen, die die Ermittlungsakten bis zur Abgabe des Verfahrens an die Staatsanwaltschaft führen, nicht selbständig über den Akteninhalt befinden. Ermittlungsakten von Hilfsbeamten der Staatsanwaltschaft seien Akten der Staatsanwaltschaft, gleichgültig ob diese von deren Führung und dem zugrunde liegenden Ermittlungsverfahren selbst bereits Kenntnis hat oder nicht. Weiterhin wurde argumentiert, die unberechtigte, weil nicht von der Staatsanwaltschaft verfügte, Entnahme von Teilen der (staatsanwaltschaftlichen) Ermittlungsakte durch Hilfsbeamte der Staatsanwaltschaft erfülle objektiv den Tatbestand der Urkundenunterdrückung gemäß § 274 Abs. 1 Nr. 2 StGB. Auch aus diesem Grunde könne man meiner Empfehlung, die Zollfahndungsdienststellen anzuweisen, erkennungsdienstliche Unterlagen anderer Ermittlungsbehörden nicht in die Ermittlungsakte aufzunehmen oder aus dieser zu entfernen, zumindest in dieser pauschalen Form nicht folgen. Da die Ermittlungsakten beim Zollfahndungsdienst ausschließlich den Bereich der Strafverfolgung beträfen, entscheide während und nach Abschluß der Verfahren ausschließlich der Staatsanwalt über deren Inhalt.

Diese Rechtsauffassung halte ich für unzutreffend. Es geht keineswegs darum, die Sachleitungsbefugnis der Staatsanwaltschaft in Frage zu stellen. Mir ist vielmehr nach dem Bundesdatenschutzgesetz die Kontrollkompetenz für sämtliche öffentliche Stellen des Bundes, also auch für die Zollfahndungsämter und deren Zweigstellen, durch Gesetz übertragen. Diese Kompetenz, die sich auf die Erhebung, Verarbeitung und Nutzung personenbezogener Daten sowohl in Dateien als auch in Akten bezieht, habe ich ausgeübt. Bei festgestellten Mängeln im Umgang mit personenbezogenen Daten kann ich Empfehlungen oder Beanstandungen aussprechen. Insoweit kann ich den vom BMF geäußerten Zweifeln an meiner Kontrollkompetenz nicht folgen. Dies habe ich gegenüber dem Ministerium in mehreren Schreiben klargestellt und auf die Rechtslage hingewiesen.

13.4 Neapel II – Übereinkommen

Mit dem Übereinkommen über gegenseitige Amtshilfe und Zusammenarbeit der Zollverwaltungen vom 18. Dezember 1997, dem sog. Neapel II-Übereinkommen (ABl. C 24 vom 23. Januar 1998, S. 1) soll die Zusammenarbeit zwischen den Zollverwaltungen der EU-Mitgliedstaaten bei der Verhinderung, Ermittlung und Verfolgung von Zuwiderhandlungen gegen Zollvorschriften verbessert werden. Es baut auf dem 1967 von den damaligen Mitgliedstaaten der Europäischen Wirtschaftsgemeinschaft vereinbarten Übereinkommen von Neapel über gegenseitige Unterstützung ihrer Zollverwaltungen auf und wurde am 18. Dezember 1997 in Brüssel unterzeichnet.

Die Beratungen über dieses neue Übereinkommen waren bereits 1990 aufgenommen worden. Erste Entwürfe umfaßten auch Vorschläge für ein Zollinformationssystem (ZIS). Die Einrichtung eines Zollinformationssystems der EU-Mitgliedstaaten wurde letztlich gesondert im Übereinkommen über den Einsatz der Informationstechnologie im Zollbereich (ZIS-Übereinkommen vom 29. Juli 1995, ABl. C 316 vom 27. November 1995, S. 33; s. u. Nr. 13.5) geregelt.

Die Mitgliedstaaten sehen das Neapel II-Übereinkommen als wichtigen Beitrag insbesondere zur Bekämpfung der organisierten Wirtschafts- und Finanzkriminalität, deren betrügerische Aktivitäten jährlich zu Einnahmeausfällen der EU in mehrfacher Milliardenhöhe und zu Fehlleitungen von EU-Subventionen in ebenfalls sehr hohem Umfang führen.

Zu diesem Zweck sieht das Übereinkommen *„besondere Formen der Zusammenarbeit“* der europäischen Zollverwaltungen vor, die das frühere Übereinkommen von 1967 in dieser Form noch nicht kannte. Das neue Übereinkommen erlaubt u. a. die grenzüberschreitende Durchführung kontrollierter Lieferungen (eine Ermittlungstechnik, die der z. B. illegale Sendungen von Waren nicht beschlagnahmt, sondern bis zum Bestimmungsort überwacht werden) und verdeckter Ermittlungen sowie die Einsetzung gemeinsamer Ermittlungsteams (Artikel 19 bis 24). Insbesondere die ebenfalls vorgesehene grenzüberschreitende Nacheile und Observation und die Durchführung verdeckter Ermittlungen durch Beamte eines EU-Mitgliedstaates auf fremdem Territorium waren vor rd. 30 Jahren noch kaum vorstellbar, da hier der Kernbereich nationaler Souveränität berührt ist. Die Mitgliedstaaten haben sich auch aus diesem Grunde nicht von Anfang an in einem genau festgelegten Umfang gegenüber den anderen Unterzeichnerstaaten zur unbeschränkten Zulassung oder Teilnahme an besonderen Formen der Zusammenarbeit verpflichtet. Das Übereinkommen erlaubt ein sog. opting out durch entsprechende Erklärungen, mit denen Bediensteten der Zollverwaltungen anderer Unterzeichnerstaaten die grenzüberschreitende Nacheile, die grenzüberschreitende Observation und die Durchführung verdeckter Ermittlungen auf dem Territorium des betreffenden Staates untersagt werden können.

Besonders sensibel ist die Durchführung verdeckter Ermittlungen auf dem Territorium eines anderen Mitgliedstaats (Artikel 23). Derartige Ermittlungen sind zeitlich begrenzt; ihre Vorbereitung und Leitung sollen in enger Zusammenarbeit zwischen den beteiligten Behörden des ersuchten und ersuchenden Mitgliedstaates erfolgen. Wichtig ist die Regelung, wonach sowohl die Bedingungen, unter denen solche Ermittlungen zulässig sind, als auch die Bedingungen, unter denen sie durchgeführt werden, also das „Ob“ und das „Wie“ verdeckter Ermittlungen im europäischen Nachbarstaat, sich nach dessen Strafprozeßrecht zu richten haben (Artikel 23 Abs. 1). Sofern bei verdeckten Ermittlungen Zufalls-

funde bezüglich anderer Zuwiderhandlungen gefunden werden, die nicht Gegenstand des ursprünglichen Ersuchens waren, werden die Bedingungen für die Verwertung dieser Informationen durch den ausländischen verdeckten Ermittler und seine nationale Zollbehörde sowie durch die ersuchte Behörde (das ist die zuständige Zollfahndungsbehörde des Mitgliedstaates, in dem verdeckt ermittelt wurde) nach deren nationalem Recht festgelegt.

Mit Blick auf die jedenfalls bisher noch nicht sehr häufige Inanspruchnahme der Möglichkeiten zur grenzschutzüberschreitenden Observation und Nacheile bleibt abzuwarten, wie oft und intensiv die Zollbehörden von den Befugnissen nach dem Neapel II-Übereinkommen Gebrauch machen werden.

Wichtige allgemeine Bestimmungen zum Datenschutz enthält Artikel 25 des Übereinkommens. Diese Bestimmung regelt den Schutz personenbezogener Daten, die von den Zollverwaltungen im Rahmen dieses Vertrags, also außerhalb des ZIS, ausgetauscht werden. Erwähnenswert in diesem Zusammenhang sind insbesondere das Recht eines Betroffenen auf Auskunft oder Berichtigung sowie die Verpflichtung zur Löschung im Falle einer unrechtmäßigen Übermittlung von einem an einen anderen Mitgliedstaat. Ferner dürfen die Daten durch die Behörden, an die die Daten übermittelt wurden, nur zweckgebunden verarbeitet werden.

Für die datenschutzrechtliche Kontrolle ist nach dem Artikel 25 des Übereinkommens die nationale Aufsichtsbehörde, für den Bereich der deutschen Zollfahndungsbehörden also meine Dienststelle zuständig.

Das Übereinkommen soll nach der Ratifizierung durch die Mitgliedsstaaten in Kraft treten. Der Entwurf eines Vertragsgesetzes nach Artikel 59 Abs. 2 GG lag mir allerdings bei Redaktionsschluß noch nicht vor.

13.5 ZIS-Übereinkommen

Schon im 14. (Nr. 26.3), 15. (Nr. 25.2) und 16. TB (Nr. 13.4.1) hatte ich über die Planungen für Zollinformationssysteme der EU-Mitgliedstaaten und der EU selbst berichtet.

Die EG Amtshilfe-Verordnung Nr. 515/97 des Rates als Rechtsgrundlage eines EG-Zollinformationssystems im Rahmen des gemeinsamen Binnenmarktes – EG-ZIS – wurde am 13. März 1997 verabschiedet. Die Verordnung regelt die Amtshilfe und Zusammenarbeit bei der Ermittlung von Zuwiderhandlungen gegen die **gemeinschaftlichen Zollvorschriften**. Demgegenüber sieht das Übereinkommen über den Einsatz der Informationstechnologie im Zollbereich vom 26. Juli 1995 ein gemeinsames Zollinformationssystem der EU-Mitgliedstaaten – ZIS – vor, das der Verhinderung, Ermittlung und Verfolgung schwerer Verstöße gegen **einzelstaatliche Regelungen** auf dem Gebiet des Zollwesens dient. Die Vorbereitung des hierzu gemäß Artikel 59 Abs. 2 GG notwendigen Vertragsgesetzes wird u. a. dadurch erschwert, daß die von mir bereits seit längerem angemahnten, auch unabhängig von der Umsetzung des ZIS-Übereinkommens erforderlichen bereichsspezifischen Datenschutzregelungen für die Zollfahndungsbehörden (s. o. Nr. 13.1) immer noch fehlen. Die vom Europäischen Rat noch im Juni 1997 angestrebte Umsetzung des ZIS-Übereinkommens bis Ende 1998 war schon aus diesem Grunde auf nationaler Ebene nicht möglich. Es ist zu hoffen, daß es jedenfalls im Laufe des Jahres 1999 möglich sein wird, auch die unabhängig von der Umsetzung des ZIS-Übereinkommens erforderlichen, grundlegenden datenschutzrechtlichen Regelungen für das Zollkriminalamt und den übrigen Zollfahndungsdienst zu schaffen (s. o. Nr. 13.1).

Die Umsetzung des ZIS-Übereinkommens wird allerdings nicht nur durch die vorerwähnten Probleme erschwert, sondern auch durch die in den Ratsgremien erörterten Vorschläge für Nachbesserungen, Ergänzungen und andere Modifikationen des Übereinkommens. Die vorgesehenen zu speichernden Daten und die Terminologie des Übereinkommens über den Einsatz der Informationstechnologie im Zollbereich (ZIS-Übereinkommen), der Verordnung (EG) Nr. 515/97 und des Neapel-II-Übereinkommens (s. o. Nr. 13.4) bedürfen noch der Feinabstimmung. So ist es z. B. aufgrund der EG-Verordnung Nr. 515/97 zulässig, im EG-ZIS amtliche Kennzeichen von Fahrzeugen (Transportmittel) zu speichern, während das ZIS-Übereinkommen derartige Speicherungen im ZIS der EU-Mitgliedstaaten bisher nicht vorsieht. Der Rat hat diese Regelungslücke im Juli 1998 erkannt und sich für eine entsprechende Erweiterung des ZIS-Übereinkommens ausgesprochen. Ferner soll im ZIS-Übereinkommen wie auch im Neapel-II-Übereinkommen ein einheitlicher Begriff der Geldwäsche verwendet werden, um sowohl den Informationsaustausch im Rahmen der „klassischen Amtshilfe“ als auch den automatisierten Informationsaustausch effektiv zu gestalten.

Bestrebungen der britischen Regierung im Rat der EU, die im ZIS der EU-Mitgliedstaaten zu speichernden Daten ohne entsprechende Änderung des Übereinkommens zu erweitern, sind aus datenschutzrechtlicher Sicht zurückzuweisen. Mit dem BMF bin ich der Auffassung, daß eine „Umwidmung“ dieses Zollinformationssystems der Mitgliedstaaten zu einer „Falldatenbank“ mit Elementen einer Recherchedatei auf administrativem Wege, d. h. ohne die erforderliche Änderung des ZIS-Übereinkommens und der nationalen Vertragsgesetze – soweit schon verkündet – nicht hinnehmbar ist. Auch mit Blick auf die im Detail noch nicht abschließend geklärte Abgrenzung der Funktionen des EG-ZIS und des ZIS der EU- Mitgliedstaaten sind zusätzliche Unklarheiten hinsichtlich der Zweckbestimmung und Funktion des ZIS der EU-Mitgliedstaaten unbedingt zu vermeiden. Man sollte vielmehr das Inkrafttreten dieses Übereinkommens und die anschließende Aufnahme des Wirkbetriebes der Datenbank abwarten, damit die gemeinsame Aufsichtsbehörde nach Artikel 18 des Übereinkommens sich mit den datenschutzrechtlichen Fragen einer möglichen Änderung befassen kann.

14 Verfassungsschutz

14.1 Gefährdung der nachrichtendienstlichen Verbindungen des BfV durch datenschutzrechtliche Kontrollen?

Bei Kontrollen der Nachrichtendienste bleibt es nicht aus, daß meine Mitarbeiter auch Kenntnis von nachrichtendienstlichen Operationen erhalten. Diese Mitarbeiter sind bis zur höchsten Stufe sicherheitsüberprüft und damit zum Umgang mit Verschlußsachen bis einschließlich der Stufe „streng geheim“ ermächtigt. Auf der anderen Seite haben die Nachrichtendienste – aus nachvollziehbaren Gründen – ein Interesse daran, daß möglichst wenige Personen Detailkenntnisse von laufenden Operationen, insbesondere von personenbezogenen Daten verdeckter Mitarbeiter oder sonstiger Informanten, Quellen oder Hilfspersonen, erlangen. Je größer die Zahl der Mitwisser in solchen Fällen ist, desto höher ist das Risiko, daß solche Quellen enttarnt werden und in Lebensgefahr bzw. sonstige Gefahrenlagen geraten könnten. Dieser Einsicht verschließe ich mich nicht. Mit diesem Argument darf jedoch meine gesetzliche Verpflichtung zur Kontrolle von Bundesbehörden nicht unmöglich gemacht werden. Da meinen Mitarbeitern jedoch in verschiedenen Fällen komplette Akten nicht vorgelegt wurden, habe ich nunmehr mit dem BfV folgende Vereinbarung getroffen, um meiner Aufgabe effektiv nachkommen zu können:

1. Meinen Mitarbeitern werden die vollständigen Akten – einschließlich sämtlicher Quellenmeldungen – gezeigt, damit sie sich einen Eindruck vom Gesamtumfang der jeweiligen Akte machen können.
2. Das BfV entnimmt daraufhin den Akten diejenigen Quellenteile, gegen deren Kenntnisnahme durch meine Mitarbeiter aus Sicht des BfV erhebliche Bedenken bestehen.
3. Meine Mitarbeiter prüfen, ob sie sich auch ohne Kenntnis von Details aus dem entnommenen Quellenteil ein Urteil über die datenschutzrechtliche Zulässigkeit des Umgangs mit den personenbezogenen Daten bilden können.
4. Soweit dies nicht möglich ist, trägt die Fachabteilung des BfV den Inhalt der quellengeschützten Aktenbestandteile mündlich vor, ohne dabei die Identität der Quellen preiszugeben.
5. Sollte es meinen Mitarbeitern im Einzelfall dennoch nicht möglich sein, die Rechtmäßigkeit des Umgangs mit den personenbezogenen Daten festzustellen, oder sollten sonstige Zweifel bestehen, wird die komplette Akte einschließlich aller Quellenteile mir persönlich vorgelegt. Ich sehe dann die komplette Akte ein und stelle selbst fest, ob ein Datenschutzverstoß vorliegt.

Dieses etwas kompliziert anmutende Verfahren wendet das BfV an, um zu vermeiden, daß es zu häufig von der sog. Staatswohlklausel Gebrauch machen muß. Nach dieser Regelung in § 24 Abs. 4 Satz 4 BDSG können Sicherheitsbehörden mir und meinen schriftlich besonders beauftragten Mitarbeitern im Einzelfall Auskunft oder Einsicht verweigern, wenn dadurch die Sicherheit des Bundes oder eines Landes gefährdet würde. Dies müßte jedoch von der obersten Bundesbehörde – hier dem BMI – im Einzelfall festgestellt werden. Um zu vermeiden, daß solche Verfahren zu oft durchgeführt werden müssen, und um gleichwohl möglichst optimal kontrollieren zu können, habe ich mich auf die vorgenannte abgestufte Vereinbarung eingelassen. Zu erwähnen bleibt jedoch, daß das BfV – und teilweise auch der BND – derartige Vereinbarungen zum Quellenschutz für erforderlich halten, während der MAD sowie einige Landesämter für Verfassungsschutz, die sich ebenfalls nachrichtendienstlicher Verbindungen bedienen, keine Bedenken haben, daß in der höchsten Stufe sicherheitsüberprüfte Mitarbeiter von Datenschutzbeauftragten quellengeschützte Informationen zur Kenntnis nehmen. In der Praxis ist bisher aber noch immer eine ausreichende Kontrolle durch mich oder meine Mitarbeiter möglich gewesen, wenn auch meine Aufgabe dadurch deutlich erschwert wird.

14.2 Akustische Wohnraumüberwachung durch das BfV nur mit richterlicher Anordnung

Mit dem Gesetz zur Änderung des Artikel 13 des Grundgesetzes vom 26. März 1998 (BGBl. I S. 610) ist für die Nachrichtendienste eine neue Situation eingetreten, da sie, was ich sehr begrüße, für Abhörmaßnahmen in Wohnungen nunmehr eine richterliche Anordnung einholen müssen. Denn für die Dienste wurde keine Ausnahmeregelung in Artikel 13 GG vorgesehen. Das BVerfSchG, das heimliches Mithören oder Aufzeichnen des in einer Wohnung nicht öffentlich gesprochenen Wortes mit technischen Mitteln zuläßt, wenn es im Einzelfall zur Abwehr einer gegenwärtigen gemeinen Gefahr oder einer gegenwärtigen Lebensgefahr für einzelne Personen unerläßlich ist und geeignete polizeiliche Hilfe für das bedrohte Rechtsgut nicht rechtzeitig erlangt werden kann, setzt bislang keine richterliche Anordnung voraus. Es fordert lediglich, die parlamentarische Kontrollkommission zu unterrichten und den Eingriff nach seiner Beendigung dem Betroffenen mitzuteilen, sobald eine Gefährdung des Zwecks des Eingriffes ausgeschlossen werden kann. Das Gesetz muß nunmehr dem neuen Artikel 13 GG angepaßt werden, weswegen ich mich an das BMI gewandt habe. Das BMI teilte mir mit, daß es aufgrund der Änderung des Grundgesetzes das BfV mit Erlaß vom selben Tage angewiesen habe, § 9 Abs. 2 BVerfSchG – bis zu seiner notwendigen Änderung – verfassungskonform anzuwenden. Danach muß das BfV nun bei entsprechenden Maßnahmen unverzüglich eine richterliche Entscheidung herbeiführen (s. auch Nr. 6.1).

14.3 Bundesverwaltungsgericht beurteilt Datenweitergabe durch BfV an private Stellen als unverhältnismäßig

In meinem 14. TB (Nr. 27.2 erster Spiegelstrich) hatte ich über ein beim Bundesverwaltungsgericht anhängiges Revisionsverfahren berichtet. Inzwischen liegt das Endurteil in der Sache vor, womit die Revision des BfV gegen das Urteil des OVG Münster aus dem Jahr 1994

zurückgewiesen wird. Hintergrund war, daß ein Mitarbeiter des BfV im Oktober 1990 den Personalchef der Klägerin aufgesucht und deren Beziehung zu Personen aus dem RAF-Umfeld erwähnt hatte. Dabei hatte er deutlich gemacht, daß es sich bei diesen Beziehungen um reine Sozialkontakte ohne politischen Hintergrund handeln könnte. Das BfV versuchte im Februar 1991, mit der Betroffenen ein Gespräch im Betrieb ihres Arbeitgebers zu führen. Die Betroffene brach das Gespräch jedoch sofort ab. Über den Gesprächsverlauf unterrichtete das BfV den Personalchef. Auf Wunsch der Firma wurde daraufhin das Arbeitsverhältnis „einvernehmlich“ zum Ende des Monats aufgelöst.

Gegen die Preisgabe ihrer personenbezogenen Daten gegenüber dem Arbeitgeber richtete sich die Klage der Betroffenen auf Feststellung, daß das Verhalten des BfV rechtswidrig war. Der Klage war sowohl vom Verwaltungsgericht als auch – nach Berufung des BfV – vom OVG stattgegeben worden. Inzwischen hat das Bundesverwaltungsgericht letztinstanzlich die Revision des BfV hiergegen zurückgewiesen. Somit steht rechtskräftig fest, daß die Weitergabe von Informationen über die Betroffene durch Mitarbeiter des BfV an den Arbeitgeber rechtswidrig war.

Während das OVG in seinen Urteilsgründen noch in Frage gestellt hatte, ob überhaupt eine Rechtsgrundlage für die offene Datenerhebung des BfV besteht, hat das Revisionsgericht zu dieser Frage nicht Stellung genommen, sondern sein Urteil ausschließlich damit begründet, das BfV habe den Grundsatz der Verhältnismäßigkeit verletzt und von mehreren Maßnahmen nicht diejenige gewählt, die die Betroffene voraussichtlich am wenigsten belastet.

Nach dieser Entscheidung wird das BfV künftig unter anderen Voraussetzungen entscheiden, ob es – u. a. wegen der Folgen für den Betroffenen – offen auftreten kann. Ich habe – in Anbetracht der immer noch umstrittenen Grundsatzfrage – das BMI aufgefordert, auf eine Änderung des BVerfSchG und die Aufnahme einer zumindest klarstellenden Regelung, wie sie in einigen Länderverfassungsschutzgesetzen enthalten ist, hinzuwirken. So schreiben einige Landesverfassungsschutzgesetze vor, daß personenbezogene Daten durch Verfassungsschutzbehörden an private Stellen nur weitergegeben werden dürfen, wenn dies **unerläßlich** ist. Die schutzwürdigen Belange des Betroffenen dürfen durch die Weitergabe nur beeinträchtigt werden, wenn dies **unvermeidbar** ist. Das BMI hat eine solche Änderung des BVerfSchG ebenfalls für wünschenswert erklärt, die aber in der 13. Legislaturperiode nicht mehr möglich war. Ich gehe davon aus, daß die Bundesregierung nunmehr kurzfristig einen Entwurf zur Änderung des BVerfSchG vorlegen wird.

14.4 Bundesamt für Verfassungsschutz erschwert Einzelfallkontrolle

Eine ausländische Mitbürgerin wandte sich an mich, nachdem sie von Mitarbeitern des BfV angesprochen worden war, die sie zur Zusammenarbeit bewegen wollten. Sie gab an, das Ansinnen des BfV sofort klar und unmißverständlich abgelehnt zu haben. Dennoch sei sie noch mehrere Stunden lang deutlich merkbar beobachtet worden. Dabei konnte sie mir die Kfz-Kennzeichen der eingesetzten Fahrzeuge angeben. In der Nähe ihrer Arbeitsstelle sei etwa einen Tag später noch einmal eine Ansprache versucht worden. Als Arbeitskollegen hinzukamen, hätten die Mitarbeiter des BfV den Anbahnungsversuch abgebrochen.

Daraufhin bat mich die Petentin um Überprüfung des Umgangs mit ihren personenbezogenen Daten beim BfV. Über die näheren Umstände des Falles kann ich hier aus Gründen des Geheimschutzes keine Ausführungen machen. Das BfV hat den Anbahnungsversuch eingeräumt und mir Unterlagen darüber zugänglich gemacht. Wie sich später herausstellte, waren diese Unterlagen unvollständig. Personenbezogene Daten über diesen Anbahnungsversuch wurden eigens in einer operativen Datei gespeichert. Erst auf intensives Nachfragen wurde diese Datenspeicherung zugegeben. Die vollständigen Daten und Unterlagen wollte mir die zuständige Fachabteilung des BfV zunächst nicht vorlegen. Dazu war erst eine Entscheidung der Leitung des BfV notwendig, die schließlich einlenkte.

Nach Einsicht in die vollständigen Unterlagen kam ich zu der Überzeugung, daß sie nicht weiter aufbewahrt zu werden brauchten, zumal auch nicht beabsichtigt war, die Petentin erneut anzusprechen. Nachdem sich das BfV zunächst auf den Standpunkt stellte, die Speicherung sei erforderlich, damit die Petentin nicht nochmals von anderen Verfassungsschutzbehörden angesprochen werde, hat es sich dann doch mit der Löschung der Daten über den Anbahnungsversuch sowie der Vernichtung der entsprechenden Unterlagen einverstanden erklärt. Die Vernichtung sei aber nur möglich, wenn sich die Petentin ausdrücklich damit einverstanden erkläre. Damit wollte das BfV dem Vorwurf vorgreifen, es habe die Akten vorzeitig vernichtet, und so eine rechtliche Prüfung unmöglich gemacht. Diese Verfahrensweise entspricht grundsätzlich meinen Forderungen.

Die Petentin hat mir auf Nachfrage telefonisch mitgeteilt, sie wolle sich zunächst an das G-10-Gremium wenden, da sie vermute, auch ihr Telefon sei durch das BfV abgehört worden. Erst wenn sie einen Bescheid von dort erhalten habe, wolle sie mir mitteilen, ob sie mit der Vernichtung ihrer Unterlagen und der Löschung der Daten einverstanden sei.

Bis dahin bleibt die Akte – wie mit dem BfV abgesprochen – gesperrt und im Gewahrsam des behördlichen Datenschutzbeauftragten. Bis Redaktionsschluß hat sich die Petentin noch nicht wieder gemeldet.

Ich finde es unverständlich, daß in den meinen Mitarbeitern vorgelegten Unterlagen kein Hinweis auf eine operative Datei und die zugehörigen Akten enthalten war und auch kein sonstiger Hinweis seitens des BfV erfolgte. Auch bedauere ich, daß eine Vorlage dieser Akten und Daten nicht sofort möglich war, sondern zunächst eine Entscheidung der Leitung eingeholt werden mußte. Es wäre jedoch wünschenswert, wenn die Mitarbeiter der

Fachabteilungen über den Umfang meiner Kontrollkompetenz besser informiert wären. Es ist aber zu begrüßen, daß die betreffenden Daten und Unterlagen zumindest gesperrt wurden und sich die Akte bis zur endgültigen Klärung in der Obhut des Datenschutzbeauftragten des BfV befindet.

14.5 Sind deutsche Hooligans Rechtsextremisten?

Nachdem bei der Fußballweltmeisterschaft 1998 in Frankreich deutsche Hooligans einen französischen Polizeibeamten lebensgefährlich verletzt hatten, trat das BfV mit der dringenden Frage an mich heran, ob auch ich es datenschutzrechtlich vertreten könnte, wenn ein Teilbestand der beim LKA Nordrhein-Westfalen bundesweit vorgehaltenen Hooligandatei der Zentralen Informationsstelle für Sporteinsätze mit NADIS abgeglichen würde. Mit dem Abgleich sollte festgestellt werden, ob Hooligans gleichzeitig als Extremisten, insbesondere als Rechtsextremisten, in Erscheinung getreten sind. Die so genommenen Datensätze sollten als Ansatz für weitere Ermittlungen dienen, um erneuten gewalttätigen Übergriffen von Hooligans bei der Fußballweltmeisterschaft in Frankreich vorzubeugen. Hintergrund der beabsichtigten Maßnahme waren u. a. auch Vorwürfe, daß durch frühzeitige Weitergabe solcher Erkenntnisse der schwere Anschlag in Frankreich hätte vermieden werden können.

In Anbetracht der brisanten Situation und der zu befürchtenden weiteren gewalttätigen Auseinandersetzungen während der Weltmeisterschaft habe ich ausnahmsweise einer weiten Auslegung der einschlägigen Regelungen des BVerfSchG zugestimmt und akzeptiert, daß das BfV das LKA Nordrhein-Westfalen um Übermittlung der für diesen Abgleich erforderlichen Daten ersucht. Es wurde vereinbart, daß die Übermittlung sowie der vollständige Datenabgleich unter Aufsicht meiner Mitarbeiter erfolgen sollten.

Wegen der Dringlichkeit habe ich umgehend Mitarbeiter zum BfV entsandt, um dort den Abgleich zu kontrollieren. Bedauerlicherweise war bei ihrem Eintreffen der Briefumschlag, in dem sich die Diskette mit personenbezogenen Daten auffällig gewordener gewaltbereiter Hooligans befand, bereits geöffnet und die Diskette auf Viren überprüft worden. Auf der Diskette waren in einer Excel-Datei enthalten: Familienname, Vorname, Geschlecht, Geburtsdatum und Geburtsort sowie eine laufende Nummer je Datensatz.

Das zu diesem Zweck vom BfV geschriebene Vergleichsprogramm zeigte auch ähnlich geschriebene Namen als Treffer an, was eine relativ hohe Übereinstimmung ergab. Die vorläufigen Treffer wurden in einer gesonderten Datei gespeichert und die Diskette des Landes Nordrhein-Westfalen mit sämtlichen Daten unter Aufsicht meiner Mitarbeiter vernichtet. Ob die Datensätze, die als Treffer gewertet wurden, tatsächlich identisch mit den Extremistendatensätzen waren, sollte unverzüglich verifiziert werden.

Nach einem Monat habe ich den Umgang des BfV mit den Ergebnissen des Datenabgleichs kontrolliert und dabei leider feststellen müssen, daß zu den meisten der von mir geprüften Fälle noch immer nicht feststand, ob die Hooligandaten mit den als Treffer zugeordneten Extremistendaten tatsächlich identisch waren. Das vorgebrachte Argument, daß die deutsche Nationalmannschaft bei der Fußballweltmeisterschaft vorzeitig ausschied, kann diese schleppende Bearbeitung nicht rechtfertigen. Unabhängig vom Ausgang der Weltmeisterschaft bin ich von der unverzüglichen Löschung der nicht mehr benötigten personenbezogenen Daten ausgegangen. Mein Unverständnis über das Verfahren habe ich in einem Schreiben dem Präsidenten des BfV mitgeteilt. Von der Leitung des BfV wurde mir daraufhin geantwortet, eine eingehende Prüfung habe ergeben, daß nur bei etwa 5,5 v. H. der von der vom LKA übermittelten Daten ein rechtsextremistischer Hintergrund bestehe. Das BfV habe in mehr als der Hälfte der verbliebenen Trefferfälle auch seine im NADIS gespeicherten Daten gelöscht. Zu einigen Fällen blieben jedoch zusätzliche Speicherungen der Landesämter für Verfassungsschutz bestehen. Bedauerlich ist, daß dem BfV offenbar erst durch diesen Abgleich aufgefallen ist, daß mehr als die Hälfte der hier überprüften personenbezogenen Daten nicht erforderlich war.

Ich habe beim BfV daraufhin eine regelmäßige Datenpflege und insbesondere eine Prüfung der Erforderlichkeit der Speicherung angemahnt und nochmals die Frage aufgeworfen, aus welchen fachlichen Gründen das BfV die Kenntnis benötigt, ob Personen, die als extremistisch eingestuft wurden, auch als Hooligans polizeilich in Erscheinung getreten sind. Im Hinblick darauf, daß das Ergebnis des Datenabgleichs auch an das LKA übermittelt werden soll, habe ich auch Zweifel geäußert, ob die Kenntnis, welche Hooligans im Zusammenhang mit möglichen extremistischen Aktivitäten auch schon vom BfV erfaßt wurden, für die polizeiliche Arbeit von Bedeutung ist. Diese Zweifel ergeben sich aus dem Trennungsgebot. Danach soll die Polizei in ihren Dateien keine Daten speichern, die sie nach den für die Polizei einschlägigen Rechtsvorschriften nicht hätte erheben dürfen. Das BfV hat mir geantwortet, diese Erkenntnisse seien für die Polizei im Rahmen ihrer Einsatzplanung zur Gefahrenabwehr erforderlich. Auf das Problem des Trennungsgebotes wurde nicht eingegangen.

In Anbetracht der langsamen – inzwischen abgeschlossenen – Folgebearbeitung vermittelt das BfV den Eindruck, als ob die dargestellte Erforderlichkeit und hohe Dringlichkeit nicht vorlagen. Ich hoffe, daß künftig solche Situationen vermieden werden.

14.6 Flächendeckende BfV-Überprüfung von Wehrpflichtigen abgewehrt

Nach verschiedenen rechtsradikalen bzw. rechtsextremistischen Vorkommnissen in der Bundeswehr ersuchte das BMVg im November 1997 das BMI und mich, nach Möglichkeiten zu suchen, wie vor der Einberufung ungedienter Wehrpflichtiger einschlägige Erkenntnisse von Verfassungsschutzbehörden auch den Kreiswehrersatzämtern mitgeteilt werden könnten. Dabei ging das BMVg davon aus, eine solche flächendeckende

Überprüfung sei bereits nach dem Wehrpflichtgesetz zulässig. Nach den von ihm angeführten Rechtsgrundlagen sei es möglich, die Nachweise dafür zu erheben, daß die Einberufung des Wehrpflichtigen keine ernstliche Gefährdung der militärischen Ordnung oder des Ansehens der Bundeswehr darstelle.

Diesen Überlegungen habe ich widersprochen. Das Verfahren käme im Ergebnis nämlich einer Regelanfrage, ähnlich dem sog. Radikalenerlaß aus den 70er Jahren, gleich. Abgesehen davon, daß das Wehrpflichtgesetz hierfür keine Rechtsgrundlage enthält, erschiene mir eine derartige Überprüfung auch unverhältnismäßig. Im System NADIS werden Daten nämlich in der Regel aufgrund nicht gerichtsfester Erkenntnisse erfaßt. Wehrpflichtige könnten also aufgrund unbestätigter Hinweise zu Verdachtspersonen werden. Die Informationen aus dem nachrichtendienstlichen Informationssystem lassen sich oft nicht so aufbereiten, daß mit hoher Wahrscheinlichkeit bewiesen werden könnte, ob der Wehrpflichtige die Voraussetzungen für die Zurückstellung nach dem Wehrpflichtgesetz erfüllt.

Auch läßt sich die Datenübermittlung vom BfV an die Kreiswehrersatzämter nicht rechtfertigen. Die Regelungen im Wehrpflichtgesetz sind so allgemein, daß sie nicht den spezialgesetzlichen Übermittlungsvorschriften des BVerfSchG vorgehen können. Das BVerfSchG sieht eine Datenübermittlung des BfV an andere Behörden auf Anfrage grundsätzlich nur in konkreten Einzelfällen vor. Einer informationellen Zusammenarbeit auf Dauer steht es entgegen. Spontanübermittlungen und Gruppenanfragen sind für derartige Fälle nicht vorgesehen. Meine ablehnende Auffassung wird auch vom BMI geteilt. Das BMVg hat daraufhin von der Regelanfrage zur Überprüfung ungedienter Wehrpflichtiger Abstand genommen.

14.7 Überprüfung der Zulässigkeit weiterer Datenspeicherungen beim BfV noch nicht abgeschlossen

Nach § 12 Abs. 3 BVerfSchG hat das BfV bei jeder Einzelfallbearbeitung, spätestens aber fünf Jahre nach der Speicherung personenbezogener Daten zu prüfen, ob diese Daten zu berichtigen oder zu löschen sind. Nach Inkrafttreten des neuen BVerfSchG vom 20. Dezember 1990 hätten solche Prüfungen eigentlich spätestens bis Ende des Jahres 1995 vorgenommen werden müssen. Wegen der großen Anzahl der gespeicherten Datensätze und der notwendigen Einsichtnahme in die Unterlagen, die die Speicherung begründen, konnten diese Überprüfungen nach Angaben des BfV auch bis Ende 1998 noch nicht endgültig abgeschlossen werden.

Das BfV hat mir auf eine entsprechende Anfrage lediglich mitgeteilt, daß die durchgeführten Überprüfungen bereits zu einer erheblichen Reduzierung der gespeicherten Datensätze geführt haben. Aus Gründen des Geheimschutzes ist es hier nicht möglich, die mir vorliegenden genauen Zahlen zu nennen. Mitteilen kann ich aber, daß sich beispielsweise im Bereich der Abteilung III (Linksextremismus/Terrorismus) die Anzahl der Datensätze um ca. 75 v. H. gegenüber den im Jahre 1990 vorhandenen reduziert hat. Auch im Bereich der Abteilung IV (Spionageabwehr, Sicherheitsüberprüfung) und der Abteilung II (Rechtsextremismus/Terrorismus) wurde der Datenbestand deutlich reduziert.

Die mit der Löschung der Daten verbundene Vernichtung der die Speicherung begründenden Unterlagen (Akten) ist in den einzelnen Abteilungen des BfV noch nicht abgeschlossen. Hinsichtlich der Abteilung V (Ausländerextremismus/Terrorismus) hat mir das BfV mitgeteilt, daß die mit der Löschung der Personendaten verbundene Vernichtung der entsprechenden Akten bis auf einen Restbestand von 150 Personenakten abgeschlossen ist. Das BfV hat zugesagt, diesen Restbestand im 1. Quartal 1999 zu bereinigen. Die Unterlagen aus Abteilung II seien hingegen bereits vernichtet.

Ich habe wiederholt gegenüber dem BfV auf einen fristgerechten Abschluß der Bereinigungsaktion gedrängt. Es sind zwar die Speicherungen in den Dateien überprüft worden, nicht aber die sonstigen Unterlagen, die die Speicherung der Daten begründen. Auch wenn die routinemäßige Überprüfung nach § 12 Abs. 3 BVerfSchG vom Wortlaut her nur die Speicherung personenbezogener Daten in Dateien umfaßt, ist es im Interesse der Betroffenen geboten, auch unverzüglich die zugrunde liegenden Unterlagen zu bereinigen bzw. zu vernichten, wenn die Prüfung zu einer Löschung der Daten aus der Datei führte. Ansonsten müßten die dort festgehaltenen Daten zumindest gesperrt werden. Das BfV ist dagegen der Auffassung, daß eine gesetzliche Verpflichtung zur Vernichtung von Akten nach Löschung der Datenspeicherung in NADIS-PZD nicht bestehe; die Arbeitspläne für die Abteilungen des BfV sehen aber dennoch grundsätzlich eine Vernichtung der Akten vor, wenn die entsprechenden Speicherungen in der PZD gelöscht sind.

15 Militärischer Abschirmdienst – MAD –

15.1 Kontrollbesuche

Nach Abschluß der Umorganisation des Militärischen Abschirmdienstes habe ich die Informationsverarbeitung beim Amt für den MAD in Köln sowie bei einer Außenstelle in Hannover 1997 kontrolliert. Mit der Umorganisation des MAD sind die bisherigen Gruppen aufgelöst und die Zahl der Mitarbeiter erheblich reduziert worden. Die Informationsverarbeitung in der Personenzentraldatei (PZD) erfolgt zentral beim MAD-Amt. Dort werden auch die entsprechenden Unterlagen aufbewahrt. Zugriff auf die gesamte PZD haben innerhalb des Amtes die Bereiche Spionageabwehr (Abteilung II) und Personeller Geheimschutz (Sicherheitsüberprüfung – Abteilung IV), während der Bereich Extremismus (Abteilung III) auf einen reduzierten Bestand zugreift. Die 14 MAD-Stellen selbst haben nur lesenden Zugriff auf einen ebenfalls reduzierten Bestand der PZD.

Im Rahmen meiner Kontrolle habe ich nach dem Zufallsprinzip eine Querschnittauswertung aus der PZD vornehmen lassen. Die hierbei ausgegebenen Personendatensätze der Abteilungen II (Extremismus), III (Spio-

nageabwehr) und IV (Personeller Geheimschutz – Sicherheitsüberprüfung) und die entsprechenden personenbezogenen Unterlagen, die diese Speicherung begründet haben, wurden umfassend überprüft. Die nachfolgend dargestellten, nicht gravierenden Verstöße gegen Datenschutzvorschriften waren zum Teil auch schon bei internen Kontrollen des Datenschutzbeauftragten des MAD-Amtes festgestellt und deren Beseitigung durch entsprechende Anweisungen der Leitung des MAD bereits eingeleitet worden.

Meine Feststellungen im einzelnen:

In mehreren Fällen – insbesondere im Bereich der Extremismusabwehr – war das Erkenntnisdatum, also das Datum des Ereignisses, das für den Beginn der Speicherfrist relevant ist (z. B. Tag der Teilnahme an einer gewalttätigen und gegen die Bundeswehr gerichteten Demonstration), falsch vergeben und somit die Frist für die Überprüfung der Löschung des Datensatzes, die nach § 7 Abs. 1 MAD-Gesetz i.V.m. § 12 Abs. 3 BVerfSchG nach fünf Jahren erfolgen muß, unzulässig lange hinausgeschoben worden. Damit blieben personenbezogene Daten länger als zulässig gespeichert. So wurde als Erkenntnisdatum z. B. statt des Datums des tatsächlichen Ereignisses der Tag des Eingangs der Meldung beim MAD-Amt eingegeben oder aber das Datum der letzten Anhörung des Betroffenen eingetragen, obwohl sich hierbei keine neuen Erkenntnisse ergeben hatten, die eine Verlängerung der Speicherfrist rechtfertigten. Das MAD-Amt hat durch entsprechende Weisungen sichergestellt, daß als Erkenntnisdatum künftig nur solche Daten eingetragen werden, die für die Bemessung der Speicherfrist tatsächlich relevant sind.

Erfreulicherweise konnte ich bei meiner Kontrolle feststellen, daß bei der Informationsverarbeitung zur Extremismusabwehr keine personenbezogenen Daten von Personen in Dateien verarbeitet werden, die der Bundeswehr nicht angehören. In den Akten des MAD-Amtes waren Angaben über diese Personen geschwärzt, wie es der Weisungslage entspricht.

Im Bereich der Abteilung IV (Personeller Geheimschutz – Sicherheitsüberprüfung) waren zahlreiche Wiedervorlagedaten deutlich später als fünf Jahre nach der letzten Bearbeitung festgesetzt worden. Dies ist darauf zurückzuführen, daß vor Inkrafttreten des MAD-Gesetzes und des Sicherheitsüberprüfungsgesetzes grundsätzlich als Wiedervorlagedatum bei Zivilpersonen das 65. Lebensjahr als Zeitpunkt für das Ausscheiden aus dem Dienst und für Soldaten das Ende der Wehrüberwachung nach dem Soldatengesetz angesetzt worden war. Nach dem Sicherheitsüberprüfungsgesetz (SÜG) von 1994 ist nunmehr vorgesehen, daß dem von einer Sicherheitsüberprüfung Betroffenen grundsätzlich nach fünf Jahren der Erklärungsbogen zur Aktualisierung zu übersenden ist. Ich halte es deswegen für geboten, daß dies zum Anlaß genommen wird, die Zulässigkeit der Speicherung sowohl beim BMVg als beantragender Stelle als auch beim MAD-Amt als mitwirkender Behörde zu überprüfen. Wie mir das BMVg mitgeteilt hat, ist eine automatisierte Bereinigung von 400 000 Datensätzen, die dann mit den zugrundeliegenden Papierunterlagen überprüft werden müßten, nicht möglich. Sie müßte manuell erfolgen, was mehrere Jahre in Anspruch nähme. Ich halte einen Verzicht auf diese Überprüfung für hinnehmbar, wenn sichergestellt ist, daß solche Datensätze, auf die im Rahmen von Wiederholungsüberprüfungen des Betroffenen wieder zugegriffen wird, entsprechend bereinigt und mit zutreffenden Wiedervorlagefristen versehen werden. Dies wurde mir zugesagt. Für neu anzulegende Datensätze ist die Vergabe zutreffender Wiedervorlagefristen inzwischen geregelt.

In einzelnen Fällen habe ich in Sicherheitsüberprüfungsakten auch noch Unterlagen gefunden, die nach der deutschen Vereinigung für künftige Sicherheitsüberprüfungen nicht mehr sicherheitserheblich sein dürften, z. B. der Besuch eines in der früheren DDR lebenden Vetters vor über 20 Jahren bei der Mutter des Sicherheitsüberprüften sowie bei ihm selbst. Diesen Besuch hatte der Betroffene selbst dem MAD mitgeteilt und war von diesem nicht als sicherheitserheblich angesehen worden. Ich habe deshalb das BMVg gebeten zu veranlassen, daß die Sicherheitsüberprüfungsakten um solche Informationen bereinigt werden. Dem ist das BMVg bisher nicht gefolgt, da es der Auffassung ist, daß auch solche Informationen, die im Verlauf einer Sicherheitsüberprüfung anfallen und zu einer Bewertung des zu Überprüfenden herangezogen wurden, nach § 18 SÜG zulässigerweise aufbewahrt werden dürften. Die Diskussion hierüber ist noch nicht abgeschlossen.

In einigen Fällen hatten die Sachbearbeiter des MAD ausführlich und nachvollziehbar begründet, daß bestimmte Akten vernichtet werden können. Dieser Entscheidungsvorschlag war durch Vorgesetzte ohne erkennbare oder nachvollziehbare Begründung jedoch aufgehoben worden. Ich kann zwar diese fachliche Entscheidung aus datenschutzrechtlicher Sicht nicht unbedingt bewerten, ich vertrete aber die Auffassung, daß bei einer Aufhebung der Entscheidung des Sachbearbeiters durch den Vorgesetzten klar erkennbar sein sollte, welche sachlichen Gründe eine weitere Aufrechterhaltung der Speicherung begründen. Dies wurde durch das BMVg zugesagt.

In einigen Akten der Abteilung II (Spionageabwehr) wurden von mir Unterlagen aus einem Disziplinarvorgang – ein strenger Verweis, weil sich der Betroffene bei seinem Vorgesetzten abgemeldet hatte, um zu Hause in Ruhe zu arbeiten, tatsächlich aber in einer Gaststätte getrunken hatte – aufgefunden, die zum Zeitpunkt des Abschlusses des Verfahrens mehr als 15 Jahre alt waren. Ich halte die weitere Aufbewahrung solcher Daten, die in der Personalakte seit langem gelöscht sein müssen, auch für Zwecke der Spionageabwehr nicht für erforderlich und habe gefordert, diese Daten aus der Akte zu entfernen. Ebenfalls gefordert habe ich, die Akten der Spionageabwehr um solche Ablichtungen von staatsanwaltschaftlichen Ermittlungsakten in Bagatellfällen einschließlich der polizeilichen Vernehmungsprotokolle und abschließender Urteile zu bereinigen, die für die weiteren Zwecke der Spionageabwehr aus meiner Sicht nicht mehr erforderlich und damit auch nicht zulässig sind. Auch dieser Forderung ist das BMVg inzwischen nachgekommen.

Leider mußte ich feststellen, daß dem MAD nicht immer mitgeteilt wurde, wenn jemand aus einer sicherheitsempfindlichen Tätigkeit oder aus der Bundeswehr ausgeschieden war. Das hatte zur Folge, daß Sicherheitsüberprüfungsunterlagen unter Umständen über die Löschungsfristen nach dem SÜG hinaus gespeichert blieben. Auch hier hat mir das BMVg zugesagt, durch geeignete Maßnahmen dafür Sorge zu sorgen, daß dem MAD diese Informationen künftig rechtzeitig und vollständig zugehen.

Im Mai 1997 habe ich die MAD-Stelle in Hannover als eine von bundesweit insgesamt 14 verbliebenen MAD-Stellen kontrolliert. Wie bereits zuvor erwähnt, hat die MAD-Stelle lediglich lesenden Zugriff auf einen eingeschränkten Datenbestand der PZD. Die bei der MAD-Stelle vorhandenen APC werden hauptsächlich für Schreibarbeiten genutzt. Bei der MAD-Stelle wird auch keine eigene Aktenhaltung betrieben. Die Erklärungsbögen der Sicherheitsüberprüfung werden nach Eingang auf Vollständigkeit geprüft, dem MAD-Amt zugeleitet und dort zentral in der PZD verarbeitet. Die Fachabteilung des MAD-Amtes beauftragt die MAD-Stelle dann mit der Durchführung der Sicherheitsüberprüfung. Die Unterlagen aus der Sicherheitsüberprüfung werden bei der MAD-Stelle lediglich bis zur Erstellung des Schlußberichts aufbewahrt und anschließend dem MAD-Amt zurückgegeben. Innerhalb der MAD-Stelle wird der zu überprüfende Fall unter der Nummer aus der PZD registriert und auch bearbeitet, eine ausdrückliche Namensregistrierung erfolgt nicht. Die von mir eingesehenen Bearbeitungsblätter über laufende und abgeschlossene Vorgänge sowie die auf der Festplatte der APC noch vorhandenen Ermittlungsberichte haben keine Anhaltspunkte dafür ergeben, daß Vorschriften nicht eingehalten wurden.

15.2 Wichtige innerdienstliche Weisung erneut ohne meine Beteiligung geändert

Bereits im März 1993 war – ohne meine vorherige Beteiligung – die neue Grundsatzweisung über die Anwendung nachrichtendienstlicher Mittel durch den MAD erlassen worden. Im Januar 1994 bemängelte ich, daß diese Weisung sich im wesentlichen auf die Wiedergabe des Gesetzestextes beschränkte. Dagegen wurde sie dem Anspruch, der Verfahrenspraxis klare Ausführungsbestimmungen an die Hand zu geben, nicht gerecht. Ich hatte gefordert, folgendes zu verdeutlichen oder als Handlungsanweisung klarzustellen:

- Vorrang gesetzlicher Zeugnisverweigerungsrechte,
- eine höhere Verhältnismäßigkeitsschwelle in bezug auf Unbeteiligte,
- Erfüllung der Voraussetzungen des Artikel 13 GG bei Eingriffen in die Unverletzlichkeit der Wohnung,
- Regelungen zur Zweckbindung und Löschung von Daten sowie zu Wiedervorlagefristen der Akten.

Mehrmals fragte ich beim BMVg an, ob und in welcher Weise beabsichtigt sei, auf meine Vorschläge und Anregungen einzugehen. Im August 1994 teilte mir das BMVg mit, diese würden im Zuge einer Überarbeitung geprüft. Nach weiteren Sachstandsanfragen meinerseits im Verlauf der Jahre 1995 und 1996 und Erwähnung des Problems in meinem 15. TB (Nr. 27.2) erhielt ich im August 1996 ein Schreiben des BMVg, wonach es einen unmittelbaren Handlungsbedarf für eine Überarbeitung dieser Grundsatzweisung nicht sehe. Im Oktober 1996 bat ich um erneute Überprüfung des Standpunktes des BMVg und erinnerte mehrfach telefonisch an die Angelegenheit. Zufällig erfuhr ich Ende des Jahres 1997, daß die Grundsatzweisung – trotz gegenteiliger Bekundungen seitens des BMVg – inzwischen geändert und mit diesen Änderungen bereits Anfang 1997 in Kraft gesetzt worden war. Im März 1998 wurde mir die aktuelle Fassung der Grundsatzweisung übersandt. Ihre Durchsicht ergab, daß meine Forderungen nicht berücksichtigt wurden, sondern ausschließlich redaktionelle Aktualisierungen erfolgt waren. Die Grundsatzweisung ist somit im wesentlichen immer noch in der von mir monierten Form in Kraft. Dies kritisiere ich besonders.

Im Hinblick auf den mittlerweile geänderten Artikel 13 GG, der jetzt auch für Abhörmaßnahmen der Nachrichtendienste in Wohnungen eine richterliche Anordnung voraussetzt (s. o. Nr. 6.1 und Nr. 14.2), gibt es nunmehr einen zwingenden Grund, die Grundsatzweisung zu überarbeiten. Hierzu habe ich das BMVg im November 1998 aufgefordert. Inzwischen hat das BMVg den MAD diesbezüglich mit einem gesonderten Erlaß angewiesen, die neue Rechtslage zu beachten. Eine gesetzliche Klarstellung hängt von der Änderung des BVerfSchG ab (vgl. Nr. 14.3), auf das im MAD-Gesetz verwiesen wird.

15.3 Kein Einsatz im sicherheitsempfindlichen Bereich wegen sexuellerAuffälligkeiten?

Anfang 1998 wandte sich ein Soldat der Bundeswehr an mich. Er bat, den Umgang mit seinen personenbezogenen Daten im Zusammenhang mit seiner Sicherheitsüberprüfung zu kontrollieren. Eine zunächst beim MAD – dieser ist mitwirkende Behörde i.S. des § 3 Abs. 2 SÜG – durchgeführte Kontrolle ergab, daß für den Soldaten bereits seit ca. fünf Jahren ein Sicherheitsbescheid (Ü2) vorlag, der zum Zugang zu Verschlußsachen bis zur Stufe „Geheim“ berechtigte. Für seine neue Verwendung im Ausland benötigte er einen Sicherheitsbescheid zum Zugang zu Verschlußsachen bis zur Stufe „Streng geheim“ bzw. „Nato Secret“ (Ü3). Hierfür wurde geprüft, ob Sicherheitsbedenken vorlagen. Diese hat der MAD nach Abschluß der Ermittlungen geäußert. Bedenken sah er insbesondere aufgrund sexueller Neigungen des Petenten und hinsichlich dessen Verschuldung. Seine sexuellen Neigungen räumte der Petent offen ein, weswegen er nicht als erpressbar gilt. Die Verschuldung war nicht übermäßig hoch, wurde vom MAD in diesem Fall jedoch als bedenklich angesehen. Den Bericht hierüber hatte der MAD dem zuständigen Geheimschutzbeauftragten beim BMVg vorgelegt. Dieser entschied aber nicht, ob dem Votum des MAD zu folgen sei. Der Betroffene war nämlich zuvor aus dem Sicherheitsbereich wegversetzt worden. Per Erlaß teilte das BMVg dem MAD diesen Umstand mit und verfügte,

dem Betroffenen dürfe ohne positiv abgeschlossene Wiederholungsüberprüfung keine sicherheitsempfindliche Tätigkeit mehr übertragen werden. Diese Weisung hat der MAD in seiner Zentraldatei gespeichert.

Anfang September 1998 überprüfte ich diesen Fall beim Geheimschutzbeauftragten des BMVg. Es bestätigte sich, daß infolge der Versetzung des Betroffenen vermieden worden war, über eine Erteilung des Sicherheitsbescheides nach Ü3 zu entscheiden. Andererseits wurde ihm durch die Entscheidung, ihn nicht mehr sicherheitsrelevant einzusetzen, auch sein Sicherheitsbescheid nach Ü2 de facto entzogen. Vor der Versetzung war er zu den Sicherheitsbedenken nicht förmlich angehört worden, obwohl § 6 SÜG dies grundsätzlich vorschreibt.

Ob die Sicherheitsbedenken gegen den Betroffenen berechtigt waren, kann hier dahinstehen. Ich habe das Verfahren jedenfalls als unzulässige Umgehung des in § 6 SÜG konkretisierten Anspruchs auf rechtliches Gehör gemäß § 25 BDSG förmlich beanstandet. Die Entscheidung, den Petenten nicht mehr bzw. nur noch unter bestimmten Voraussetzungen im sicherheitsempfindlichen Bereich einzusetzen, stellt für ihn eine Beschwer dar, denn seine Verwendbarkeit ist damit eingeschränkt. Es spielt insoweit keine Rolle, ob ihm anläßlich einer Wiederholungsüberprüfung rechtliches Gehör gewährt worden wäre, wie das BMVg erklärte. Allein die Tatsache, daß über ihn in der Sicherheitsakte und in der Sicherheitsüberprüfungsakte ein Erlaß des BMVg vorliegt, der Sicherheitsbedenken erkennen läßt, stellt eine negative Entscheidung dar. Ihm hätte Gelegenheit zur Stellungnahme gegeben werden müssen, damit er die Möglichkeit erhielt, vermutete Sicherheitsbedenken gegebenenfalls auszuräumen.

Außerdem habe ich dem BMVg mitgeteilt, daß ich für die Speicherung der Weisung des Geheimschutzbeauftragten in der Zentraldatei des MAD keine Rechtsgrundlage sehe. In § 20 Abs. 2 Satz 1 SÜG sind die personenbezogenen Daten, die von Behörden nach diesem Gesetz gespeichert werden dürfen, enumerativ aufgezählt. Die Speicherung der Weisung geht über diese zulässigen personenbezogenen Daten hinaus.

In seiner Gegenäußerung stellt sich das BMVg auf den formalen Standpunkt, da der Betroffene keine sicherheitsempfindliche Tätigkeit mehr ausübe, bedürfe er auch keiner Sicherheitsermächtigung. Daher sei auch kein Nachteil zu entdecken. Das BMVg übersieht aber die faktischen Auswirkungen für den Betroffenen.

Da nicht auszuschließen ist, daß in vergleichbaren Fällen ähnlich verfahren wird, halte ich meine Beanstandung aufrecht.

16 Bundesnachrichtendienst

16.1 Altdaten endlich bereinigt; Datenverarbeitung zum Teil immer noch ohne vorgeschriebene Dateianordnungen

Bereits in meinem 16. TB (Nr. 16.2, letzter Absatz) hatte ich über die Zusage des BND berichtet, seine Altdatenbestände zu bereinigen. Diese Bereinigung alter, nicht mehr erforderlicher bzw. nach dem neuen BND-Gesetz nicht mehr zulässiger Datenspeicherungen hätte bis spätestens fünf Jahre nach Inkrafttreten des neuen BND-Gesetzes vom 20. Dezember 1990 abgeschlossen sein müssen. Das BND-Gesetz schreibt – wie das BVerfSchG – nämlich vor, daß personenbezogene Daten bei jeder Einzelfallbearbeitung, spätestens aber nach fünf Jahren auf ihre Richtigkeit und Erforderlichkeit hin zu überprüfen sind. Aufgrund verschiedener organisatorischer Probleme und vordringlicher anderer Aufgaben des BND hatte ich mich mit einer kurzen Überschreitung dieser Frist einverstanden erklärt. Nachdem die Frist mehrfach nicht eingehalten werden konnte, hat mir der BND im Februar 1998 den Abschluß der Überprüfung und die Löschung überflüssiger bzw. unzulässiger Daten mitgeteilt. Danach hat der BND seit 1991 den Datenbestand in seiner zentralen Datei auf nur noch ca. ein Drittel der früheren Datenmenge reduziert. Zu diesem erfreulichen Ergebnis kam es trotz zahlreicher neuer Speicherungen während desselben Zeitraumes. Ich gehe davon aus, daß die Datenbereinigung auch für die Aufgabenerfüllung des BND Vorteile hat, da mit weniger, aber dafür aktuellen und gepflegten Datenbeständen auch eine effektivere Arbeit möglich ist.

Zu meinem Bedauern hat der BND die Verpflichtung nach dem BND-Gesetz, für seine Dateien mit personenbezogenen Daten Dateianordnungen zu erstellen und mich vor deren Erlaß zu beteiligen, noch nicht erfüllt. Mir liegen zwar inzwischen einige Dateianordnungen vor, an denen ich auch beteiligt wurde, doch habe ich bei meinen Kontrollen immer wieder festgestellt, daß es zu etlichen Dateien die vorgeschriebenen Dateianordnungen noch nicht gibt. Seitens des BND sind mir jedoch inzwischen weitere Dateianordnungen angekündigt worden. Dem sehe ich mit Interesse entgegen.

16.2 Übermäßige Datenerhebung und Speicherung bei Sicherheitsüberprüfungen

Nach dem Sicherheitsüberprüfungsgesetz (SÜG) führt der BND selbst die Sicherheitsüberprüfungen von Bewerbern und Mitarbeitern des Dienstes durch. Er ist also zuständige Behörde und zugleich mitwirkende Stelle i.S. des SÜG. Hierzu sieht das SÜG vor, daß bestimmte personenbezogene Daten erhoben und teilweise auch in Dateien gespeichert werden dürfen. Neben diversen Dateiabfragen ist, abgestuft nach dem Geheimhaltungsgrad der Verschlußsachen, gegebenenfalls auch eine Identitätsprüfung erforderlich, und in bestimmten Fällen dürfen darüber hinaus auch Sicherheitsermittlungen durchgeführt werden. Das SÜG erlaubt dem BND zur Identitätsprüfung, vom Betroffenen in seiner Sicherheitserklärung benannte Referenzpersonen sowie weitere geeignete Auskunftspersonen zu befragen, ob die Angaben des Betroffenen zutreffen oder ob tatsächliche Anhaltspunkte vorliegen, die auf ein Sicherheitsrisiko schließen lassen. Mit den Dateiabfragen soll geklärt werden, ob der Betroffene z. B. bei Polizei, Nachrichtendiensten oder im Zusammenhang mit Stasi-Angelegenheiten aufgefallen ist. Zu diesen Abfragen ermächtigt das SÜG nach meiner Auffassung nur bezogen auf

den Betroffenen selbst sowie dessen ggf. in die Überprüfung einbezogenen Lebenspartner.

Wie ich bei meinen Prüfungen festgestellt habe, läßt der BND aber auch Referenz- und Auskunftspersonen beim BfV daraufhin überprüfen, ob sie dort erfaßt sind. Dazu wird das System NADIS befragt. Ich bin der Auffassung, daß das SÜG als spezialgesetzliche Grundlage für die Durchführung von Sicherheitsüberprüfungen die Maßnahmen **abschließend** aufzählt, die zu diesem Zweck getroffen werden dürfen. Ein Datenabgleich für Referenz- und Auskunftspersonen mit dem NADIS als eine Form der Datenerhebung zählt hierzu nicht.

Der BND stellt sich dagegen auf den Standpunkt, das BND-Gesetz jedenfalls erlaube diese Datenerhebungen zum Schutz seiner Mitarbeiter, Einrichtungen, Gegenstände und Quellen gegen sicherheitsgefährdende oder geheimdienstliche Tätigkeiten. Mit der gleichen Begründung werden auch weitere Datenerhebungen und Speicherungen sowie Ermittlungsmaßnahmen durchgeführt, die vom SÜG nicht vorgesehen sind. Über die Maßnahmen im einzelnen kann ich hier aus Geheimhaltungsgründen nicht berichten. Ich meine jedoch, daß Datenerhebungen über den vom SÜG vorgesehenen Rahmen hinaus nur dann auf die Regelungen des BNDG gestützt werden dürfen, wenn tatsächliche Anhaltspunkte für eine konkrete Gefahr sicherheitsgefährdender oder geheimdienstlicher Tätigkeiten bestehen.

Der BND argumentiert, es gehöre zum nachrichtendienstlichen Erfahrungswissen, daß Spione auch mit von ihnen selbst benannten Referenzpersonen zusammenarbeiteten. Ein solches nachrichtendienstliches Erfahrungswissen, das allenfalls eine abstrakte Gefahr begründen kann, vermag eine Regelanfrage zu Referenz- oder Auskunftspersonen nicht zu rechtfertigen. Hätte der Gesetzgeber gewollt, daß der BND zusätzlich zu den Maßnahmen, die das SÜG vorsieht, weitergehende Eingriffe nach dem BND-Gesetz vornehmen darf, hätte er die einschränkenden Regelungen im SÜG nicht zu treffen brauchen. Die weitergehenden Eingriffe hätte das BNDG nämlich schon vor Inkrafttreten des SÜG gerechtfertigt. Ich habe auch festgestellt, daß der BND zur Durchführung des SÜG in einer Datei sog. Volltexte gespeichert hat, was ich aber als Verstoß gegen das SÜG **beanstandet** habe.

Aufgrund meiner Intervention hat der BND das Verfahren bei der Sicherheitsüberprüfung korrigiert und führt weniger zusätzliche Dateiabfragen und Ermittlungen durch. Er hat mir einen Katalog von Maßnahmen vorgelegt, die er in bestimmten Fällen zusätzlich zu dem nach dem SÜG Erlaubten für zwingend erforderlich hält.

Da nachvollziehbar ist, daß ein Nachrichtendienst sich in besonderem Maße gegen Ausspähung schützen muß, habe ich einem Teil dieser Maßnahmen zugestimmt. An die sog. nachrichtendienstlichen Gefahren brauchen wegen des hohen Risikos auch nach meiner Auffassung geringere Anforderungen gestellt zu werden als an den im Polizeirecht üblichen Gefahrenbegriff. Mit der regelmäßigen Abfrage von Referenz- und Auskunftspersonen ohne Vorliegen zusätzlicher tatsächlicher Anhaltspunkte für eine konkrete Gefahr würde der Begriff der nachrichtendienstlichen Gefahr aber eindeutig überstrapaziert.

16.3 BND gibt beim Erkenntnisdatum nach, möchte aber sog. operative Daten nicht mehr regelmäßig überprüfen

Die Gesetze über die Nachrichtendienste sehen vor, daß die Rechtmäßigkeit der Speicherung personenbezogener Daten bei jeder Einzelfallbearbeitung, spätestens aber nach Ablauf von fünf Jahren zu überprüfen ist. Mit den Sicherheitsbehörden, insbesondere auch mit den Nachrichtendiensten (BfV und MAD) besteht Einvernehmen, daß Anknüpfungszeitpunkt für diese Überprüfung der Zeitpunkt des tatsächlichen Ereignisses ist. Nur der BND stellte sich bisher auf den Standpunkt, die fünfjährige Überprüfungsfrist beginne ab dem Zeitpunkt, zu dem diese Daten in seinen Dateien gespeichert werden. Das könnte im Extremfall bedeuten, daß z. B. eine vier, fünf oder zehn Jahre alte Information u.U. erst nach weiteren fünf Jahren auf ihre Erforderlichkeit überprüft würde. Dabei könnte sich ihre Unrichtigkeit oder mangelnde Erforderlichkeit für den BND bereits viel früher herausstellen. In diesem Punkt wurde zwischenzeitlich mit dem BND ein Verfahren gefunden, das demjenigen bei den anderen Sicherheitsbehörden entspricht. Die Regelung berücksichtigt jedoch, daß in vielen Fällen der konkrete Zeitpunkt des Ereignisses nicht mehr feststellbar sein wird.

Leider ist der BND jedoch der Auffassung, daß die gesetzlich vorgeschriebene Regelüberprüfung nach spätestens fünf Jahren, unabhängig vom Erkenntnisdatum, künftig in bestimmten Fällen nicht mehr durchgeführt werden soll. Dies begründet er damit, daß sog. operative Vorhaben, wegen deren unter Umständen langen Dauer und ihrer für den Dienst hohen Bedeutung, aber auch zur Abwehr unberechtigter Regreßansprüche – in Abweichung von der gesetzlichen Zehnjahresfrist – ohnehin nie gelöscht werden dürften. Daher sei eine regelmäßige Überprüfung im Abstand von fünf Jahren, ob die Daten gelöscht werden könnten, zwangsläufig überflüssig.

Ich bin der Auffassung, daß eine so lange Speicherung von Daten aus operativen Vorhaben nicht in jedem Falle erforderlich ist. Dies gilt insbesondere für viele der von mir geprüften Erfassungen. Im übrigen verkennt der BND, daß die regelmäßige Überprüfung im Abstand von spätestens fünf Jahren nicht nur der Klärung dient, ob die Daten gelöscht werden können, sondern auch den Zweck hat, die Daten auf ihre Richtigkeit und Aktualität zu überprüfen. Ich bin mit dem BND so verblieben, daß dieser einen Vorschlag für ein vereinfachtes Verfahren der Routineüberprüfung ausarbeitet und mir zur Abstimmung vorlegt. Wie dieses Verfahren aussehen soll, war mir bei Redaktionsschluß noch nicht bekannt.

16.4 Strategische Fernmeldeaufklärung des BND auf dem verfassungsgerichtlichen Prüfstand

Das Bundesverfassungsgericht hat am 15./16. Dezember 1998 eine mündliche Verhandlung über drei Verfassungsbeschwerden gegen die mit dem Verbrechensbekämpfungsgesetz 1994 erweiterte sog. strategische Fernmeldeaufklärung des BND durchgeführt. Über diese Überwachung des grenzüberschreitenden Fernmeldever-

kehrs habe ich bereits früher (vgl. 15. TB Nr. 28.2, 16. TB Nr. 16.1) ausführlich berichtet. An der Verhandlung habe ich gemeinsam mit mehreren Landesbeauftragten für den Datenschutz teilgenommen. Das Bundesverfassungsgericht hatte zuvor allen Beteiligten einen umfangreichen Fragenkatalog übersandt. Auch dies unterstreicht, daß das Gericht der Problematik solcher Überwachungsmaßnahmen große Bedeutung zumißt. In der Verhandlung habe ich die Rechtsauffassung vertreten, wie ich sie bereits in früheren schriftlichen Stellungnahmen gegenüber dem Gericht sowie in den parlamentarischen Beratungen über den damaligen Gesetzentwurf geäußert habe.

Die neuen Befugnisse des BND bei der Kontrolle des nicht leitungsgebundenen grenzüberschreitenden Fernmeldeverkehrs habe ich nicht grundsätzlich in Abrede gestellt, wenngleich man nach den vom BND vorgelegten Erkenntnissen zum Vollzug des Gesetzes erhebliche Zweifel an der Verhältnismäßigkeit und Geeignetheit dieser neuen Überwachungsbefugnisse hegen muß. Dem Gericht verbleibt aber die schwierige Entscheidung, ob es sich bei den Maßnahmen des BND um eine strategische, sachverhaltsbezogene Kontrolle handelt oder ob nicht doch eine Tendenz zur Individualkontrolle festzustellen ist.

Zu den weiteren datenschutzrechtlich relevanten Fragen habe ich folgende Auffassung vertreten:

- Zur Frage der Verwertung und Weitergabe personenbezogener Erkenntnisse aus der Überwachung habe ich erneut gefordert, daß zumindest „bestimmte Tatsachen“ den Verdacht begründen müßten, daß jemand Straftaten plant, begeht oder begangen hat. Dies entspricht auch der im Strafverfahrensrecht üblichen Schwelle. Diesen höheren Grad an Verdachtsverdichtung halte ich für erforderlich, damit nicht unverhältnismäßig viele Nichtbetroffene ins Visier der Sicherheitsbehörden gelangen. Denselben Maßstab hat auch das Bundesverfassungsgericht seiner Entscheidung vom 5. Juli 1995 – 1 BvR 2226/94 – über den Erlaß einer einstweiligen Anordnung zu Artikel 1 § 3 G 10-Gesetz zugrunde gelegt (Pressemitteilung des BVerfG Nr. 30/95 vom 13. Juli 1995).
- Die Entscheidung über die zweckändernde Nutzung von personenbezogenen Erkenntnissen aus der Fernmeldeaufklärung sollte einer unabhängigen Instanz, also außerhalb des BND, vorbehalten bleiben.
- Der Betroffene ist über Maßnahmen nach § 3 G 10 zu unterrichten, sobald eine Zweckgefährdung der Maßnahmen nicht mehr andauert. Sind die erlangten Daten personenbezogen verwendet worden, darf eine Mitteilung entgegen § 3 Abs. 8 Satz 2 G 10 grundsätzlich nicht unterbleiben.
- Die Erhebung und Verwendung personenbezogener Erkenntnisse aus der strategischen Fernmeldeaufklärung erfordert über die bisherige Praxis hinaus eine effektive datenschutzrechtliche Kontrolle. Dies gilt für alle Phasen der Datenverwendung, also auch bezüglich der Löschung, der Weitergabe an andere Stellen und der Mitteilung an den Betroffenen.

Der Senat gab zum Abschluß der Verhandlung bekannt, mit einer Entscheidung über die Beschwerden sei binnen drei Monaten zu rechnen. Ich erhoffe mir von der Entscheidung u. a. grundsätzliche Ausführungen zum Schutzbereich des Fernmeldegeheimnisses sowie zu einer effektiven datenschutzrechtlichen Kontrolle im G 10-Bereich.

16.5 Überarbeitung des Verfahrens zur Sicherheitsanfrage überfällig

Unabhängig von der Sicherheitsüberprüfung nach dem SÜG (vgl. Nr. 16.2) ist es in bestimmten Fällen zum Schutz des BND oder seiner Mitarbeiter, Einrichtungen und Quellen vor Ausspähung erforderlich, personenbezogene Daten anderer Personen, z. B. von Lieferanten, zu überprüfen. Für diese Dateiabfragen bei den Sicherheitsbehörden enthält das BND-Gesetz eine Rechtsgrundlage. Anläßlich meiner Kontrollen beim BND habe ich festgestellt, daß diese Möglichkeiten sehr extensiv genutzt wurden. Die interne Verfügung über solche Sicherheitsanfragen zu Personen sah eine ausufernde Zahl von Möglichkeiten vor, Personen zum Schutz des BND, seiner Mitarbeiter, Einrichtungen und Quellen zu überprüfen. Dies habe ich moniert und schon Ende 1997 vom BND die Zusage erhalten, die Verfügung zu überarbeiten. Obwohl zu dieser Verfügung grundsätzlich bereits Einvernehmen zwischen dem BND und mir bestand, ist mir trotz wiederholter Nachfrage noch immer kein Entwurf einer neuen Verfügung zugegangen. Ich habe gegenüber dem Dienst mehrfach auf die Dringlichkeit der Neuregelung hingewiesen. Er hat vor, den Entwurf der Verfügung bis Mai 1999 fertigzustellen.

17 Sicherheitsüberprüfungsgesetz

– Kontrolle bei einem Unternehmen der Rüstungsbranche ohne große Probleme –

Auch 1997 habe ich im Rahmen meiner Zuständigkeit nach dem SÜG ein Unternehmen der Privatwirtschaft kontrolliert, das rüstungsrelevante Aufträge erhält, für die seine Beschäftigten den Zugang zu sicherheitsempfindlichen Bereichen und zu Verschlußsachen benötigen und deshalb einer Sicherheitsüberprüfung zu unterziehen sind. Wie ich in meinem 16. TB (vgl. Nr. 17.4) dargestellt habe, ist mir diese Aufgabe durch das SÜG vom 20. April 1994 (BGBl. I S. 867) übertragen worden.

Bei dem Unternehmen mit damals ca. 1 330 Mitarbeitern, von denen ca. 1 050 Personen sicherheitsermächtigt waren, handelt es sich um ein Hochtechnologieunternehmen, das überwiegend wehrtechnische Aufträge bearbeitet. Damit ist auch der hohe Anteil der sicherheitsermächtigten Mitarbeiter zu erklären. Die ermächtigten Mitarbeiter sind in ihrer Mehrzahl nach Ü2 (erweiterte Sicherheitsüberprüfung) überprüft, da sie Zutritt zu verschiedenen, streng abgetrennten und mit besonderen Zugangskontrollen geschützten Sicherheitsbereichen haben und mit Verschlußsachen befaßt sind. Für den Sicherheitsbevollmächtigten selbst und die Registratoren, die die Verschlußsachen verwalten, werden Sicherheitsüberprüfungen nach Ü3 (erweiterte Sicherheitsüberprüfung mit Sicherheitsermittlungen) durchgeführt.

Das Aufgabengebiet Geheimschutzverfahren des Unternehmens ist innerhalb eines Gebäudes auf einem Stockwerk untergebracht, das nur mittels einer speziellen Codekarte zugänglich ist. Die Sicherheitsakten und der Personalcomputer, auf dem die Datenbanken mit den Daten der Sicherheitsermächtigten und der zugelassenen Besucher des Unternehmens betrieben werden, befinden sich dort in Räumen, die nochmals gesondert gesichert sind. Eine wirksame Zugangskontrolle ist somit sichergestellt. Zugriff auf die Sicherheitsakten und auf die Datenbanken haben nur der Sicherheitsbevollmächtigte und eine weitere von ihm beauftragte Person. Die Sicherheitsakten der aktuell sicherheitsermächtigten Mitarbeiter werden in verschließbaren Rollschränken aufbewahrt. Die Sicherheitsakten der ausgeschiedenen Mitarbeiter werden, nach Jahrgängen des Ausscheidens aus dem sicherheitsempfindlichen Bereich chronologisch geordnet, in einem separaten Raum, und dort ebenfalls in verschließbaren Schränken, aufbewahrt. Auch die Aktenaufbewahrung entspricht § 9 BDSG.

Die Kontrolle zahlreicher Sicherheitsakten aktuell ermächtigter Mitarbeiter hat ergeben, daß hierin grundsätzlich nur solche Unterlagen geführt werden, die nach dem SÜG zulässig sind. In einigen Sicherheitsakten fanden sich allerdings Unterlagen (z. B. Mitteilungen der Bediensteten über Reisen in die ehemalige DDR, die z. T. schon 20 Jahre oder länger zurücklagen), deren weitere Aufbewahrung nach den politischen Veränderungen und der deutschen Vereinigung aus meiner Sicht nicht mehr erforderlich sind. Das BMWi als zuständiger Geheimschutzbeauftragter vertritt aber die Ansicht, daß die Aufbewahrung dieser Unterlagen nach § 18 SÜG zulässig sei, weil sie den Verlauf von Sicherheitsüberprüfungen komplettieren und auch für weitere Sicherheitsüberprüfungen relevant sein könnten. Eine Einigung mit dem BMWi über diese Problematik konnte bisher nicht erzielt werden.

Kontrolliert habe ich auch die Sicherheitsakten von Mitarbeitern, die aus dem sicherheitsempfindlichen Bereich oder aus dem Unternehmen ganz ausgeschiedenen waren. Hier konnte ich feststellen, daß die Sicherheitsakten nach der nach dem SÜG geltenden 5-Jahresfrist ausgesondert werden, und zwar jeweils zum Jahresende. Ich habe aber auch festgestellt, daß noch Sicherheitsakten von Personen aufbewahrt wurden, die ihre Tätigkeit im sicherheitsempfindlichen Bereich gar nicht angetreten haben. Solche Akten sind nach § 30 SÜG i.V.m. § 19 Abs. 2 SÜG grundsätzlich nach einem Jahr zu vernichten. Das BMWi hat den Sicherheitsbevollmächtigten inzwischen aufgefordert, die Akten aller ausgeschiedenen Mitarbeiter auf solche Fälle durchzusehen und deren Sicherheitsakten umgehend zu vernichten. Dieser hat darüber hinaus zugesagt, die Sicherheitsakten für den betroffenen Personenkreis künftig gesondert aufzubewahren, so daß die Aussonderungsfrist besser überwacht werden kann.

Um die Aufgaben nach dem SÜG erfüllen zu können, werden zwei Datenbanken betrieben, auf die nur der Sicherheitsbevollmächtigte und eine weitere Person Zugriff haben. In einer Datenbank werden die personenbezogenen Daten der aktuell sicherheitsermächtigten Mitarbeiter des Unternehmens erfaßt. Zu jedem Betroffenen wird ein sehr umfangreicher Datensatz geführt. Diese Speicherung ist nach § 31 SÜG zulässig.

In einer zweiten Datenbank werden personenbezogene Daten von Mitarbeitern anderer Unternehmen gespeichert, die berechtigt sind, den sicherheitsempfindlichen Bereich des Unternehmens zu betreten. Darüber hinaus werden hier personenbezogene Daten von eigenen Mitarbeitern gespeichert, die eine solche Berechtigung für andere Unternehmen haben. Auch diese Datenspeicherungen sind nach § 31 SÜG zulässig.

Die Datenbanken werden auf einem nicht vernetzten PC geführt. Die getroffenen Sicherungsmaßnahmen entsprechen § 9 BDSG und der Anlage hierzu. Insoweit habe ich bei dem geprüften Unternehmen in keinem Bereich Defizite festgestellt.

18 Personaldaten

18.1 Gesetzgebung

18.1.1 Auskunftsumfang ärztlicher Gutachten bei Dienst(un)fähigkeit

Im Rahmen des „Gesetzes zur Reform des öffentlichen Dienstrechts“, auch Dienstrechts-Reformgesetz genannt, wurde beraten, die Auskunftspflicht des untersuchenden Arztes bei Dienst(un)fähigkeitsuntersuchungen im BBG wesentlich zu erweitern. Unabhängig von Willen und Kenntnis des Beamten sollte die Behörde „die maßgebenden Untersuchungsbefunde“ vom Arzt anfordern können.

Das für das öffentliche Dienstrecht zuständige BMI sah hierin lediglich eine Klarstellung, da nach geltendem Recht keine Schweigepflicht des begutachtenden Arztes gegenüber dem Dienstherrn des zu untersuchenden Beamten bestehe – eine Rechtsauffassung, der ich mit Unterstützung des BMJ stets entgegengetreten war. Das BMI war entgegen meinen Empfehlungen nicht bereit, die Übermittlungsbefugnis des Arztes lediglich auf das Untersuchungsergebnis zu beschränken, wie dies etwa im saarländischen Beamtengesetz vorgesehen ist (§ 52 Abs. 1 Satz 4).

Meine Bedenken gegen die weite Fassung des Regierungsentwurfs fußen vor allem darauf, daß der Dienstherr nicht die medizinische Fachkunde und Erfahrung besitzt, um das Gutachten des Amtsarztes zu überprüfen und etwa aus der Anamnese und den Befunden ein anderes medizinisch begründetes Ergebnis über die Dienstfähigkeit des Beamten ableiten kann. Auch die amtliche Begründung, wonach die Dienstunfähigkeit durch „die zuständige Behörde und den Arzt oder den Beamten“ in einzelnen Fällen unterschiedlich beurteilt worden war, überzeugt nicht: Der Dienstherr bekommt nicht größeren medizinischen Sachverstand, wenn ihm das vollständige Gutachten übermittelt wird. Wenn er meint, daß das Ergebnis des Amtsarztes nicht korrekt ist, kann er es nur durch ein weiteres Gutachten, das eines anderen Arztes, in Frage stellen.

Ich habe meine Auffassung dem Innenausschuß des Deutschen Bundestages ausführlich dargelegt.

Im Verlauf der Gesetzgebung sind dann auch Inhalt und Wortlaut der Übermittlungsbefugnis wesentlich verändert und als § 46a in das Bundesbeamtengesetz aufgenommen worden. Ich habe mich zwar nicht mit meinem Wunsch durchsetzen können, die Übermittlungsbefugnis auf das Untersuchungsergebnis zu beschränken. Aber die Vorschrift wurde immerhin enger gefaßt; neben dem Ergebnis dürfen nur noch „die tragenden Feststellungen und Gründe" mitgeteilt werden. Damit dürfen beispielsweise die Anamnese und medizinische Einzelbefunde, die mit dem Ergebnis nichts zu tun haben, nicht weitergegeben werden. Die Übermittlung ist auf den „Einzelfall auf Anforderung der Behörde" beschränkt, soweit die Kenntnis für die Behörde unter Beachtung des Grundsatzes der Verhältnismäßigkeit für die von ihr zu treffende Entscheidung erforderlich ist.

Große Bedeutung messe ich den in § 46a Abs. 3 BBG neu eingeführten Verfahrensvorschriften bei. Im Gegenzug zu der Übermittlungsbefugnis muß der Beamte nämlich zu Beginn der Untersuchung auf diese selbst sowie auf deren Zweck hingewiesen werden. Er weiß damit, daß die Schweigepflicht des untersuchenden Arztes gegenüber der Beschäftigungsbehörde durch § 46a BBG begrenzt ist.

Zudem erhält der Beamte eine Kopie der vom Arzt an die Behörde erteilten Auskünfte. Diese Regelung gewährleistet, daß er über den Kenntnisstand seiner Behörde nicht im Ungewissen gelassen wird, und schafft so die gebotene Transparenz. Neu gegenüber dem ursprünglichen Entwurf ist auch die klare Zweckbindung des Untersuchungsergebnisses (§ 46a Abs. 2 Satz 2 BBG).

18.1.2 Arbeitnehmerdatenschutzgesetz

In seinem Beschluß zu meinem 14. TB hatte der Deutsche Bundestag die Bundesregierung aufgefordert, den längst überfälligen Entwurf „bereichsspezifischer Regelungen zum Arbeitnehmerdatenschutz" vorzulegen. Weil sie dem nicht nachkam, hat der Deutsche Bundestag die Aufforderung im Zusammenhang mit meinem 15. TB wiederholt und der Bundesregierung eine Frist bis Ende 1997 gesetzt – geschehen ist bisher gleichwohl nichts.

In den Kreis derer, die ein Arbeitnehmerdatenschutzgesetz anmahnen, hat sich mit dem Bundesarbeitsgericht (BAG) eine weitere namhafte Stimme eingereiht. In einer vielbeachteten Entscheidung hatte es die Kontrollbefugnis des betrieblichen Datenschutzbeauftragten beim Betriebsrat im wesentlichen deswegen verneint, weil eine gesetzliche Regelungslücke bestehe (vgl. Beschluß des BAG vom 11. November 1997 (1 ABR 21/97)). Insoweit hatte sich das BAG darauf bezogen, daß *„die zuständigen Verfassungsorgane immer wieder bekundet [hatten], daß eine bereichsspezifische Regelung für den Arbeitnehmerdatenschutz zum noch unerledigten Gesetzgebungsprogramm gehört."* Das BAG hat für die von ihm zu entscheidende Fragestellung aufgezeigt, daß es durchaus Möglichkeiten für eine sachgerechte Lösung gäbe. Es sah sich jedoch an einer Entscheidung gehindert, da diese einen weitgehenden *„Eingriff in das gesetzliche Regelungsprogramm"* bedeutet hätte, was der Rechtsprechung verwehrt sei. Als Konsequenz wirft die Entscheidung des BAG allerdings neue Fragen für die Praxis auf.

Auch in anderen Bereichen des Arbeitnehmerdatenschutzes, wie z. B. Videoüberwachung am Arbeitsplatz, das Fragerecht des Arbeitgebers vor Einstellungen oder die Einschaltung von Detekteien zur Überwachung von Arbeitnehmern, besteht Rechtsunsicherheit, weil die Rechtslage aufgrund einer notwendigerweise lückenhaften, aber auch schwer zu erschließenden Rechtsprechung vielfach nicht eindeutig ist. Unabhängig hiervon ist es nicht unproblematisch, wenn mit Blick auf die deutsche Rechtsordnung Arbeitnehmer und Arbeitgeber bestimmte Rechte und Pflichten nach geltendem Recht nur noch aus der Rechtsprechung ableiten können.

Die Schaffung eines Arbeitnehmerdatenschutzgesetzes ist dringlicher denn je (zur Novellierung des BDSG und zu meinen Forderungen an den Reformgesetzgeber s. o. Nr. 2.1.2).

18.2 Erhebung von Personaldaten der Mitarbeiter

18.2.1 Übersicht über Arbeitsergebnisse von Einzelentscheidern beim Bundesamt für die Anerkennung ausländischer Flüchtlinge – Eine unendliche Geschichte

Mein Schriftverkehr mit dem BAFl über die Einführung von Arbeitsübersichten für Einzelentscheider glich in 4 Jahren einem Verwirrspiel, das schließlich in einer förmlichen Beanstandung wegen mangelnder Unterstützung meiner gesetzlichen Aufgabe endete.

Ich hatte das BAFl sowie das BMI als oberste Dienstbehörde darum gebeten, die bestehende Dienstanweisung zur Führung der Übersichten unter Beteiligung der Personalvertretung entsprechend den gesetzlichen Vorgaben anzupassen. Hierzu hatte ich Ergänzungsvorschläge, beispielsweise zur Regelung von Einsichts-, Nutzungsrechten sowie Aufbewahrungsfristen gemacht. Außerdem hatte ich nochmals darauf hingewiesen, daß neben der datenschutzrechtlichen Zulässigkeit die Genehmigung der zuständigen obersten Dienstbehörde gemäß § 90 Abs. 4 Satz 2 BBG – was für Angestellte und Arbeiter öffentlicher Arbeitgeber des Bundes sinngemäß anzuwenden ist (vgl. 15. TB Nr. 9.13) – einzuholen und das Mitbestimmungsverfahren mit der Personalvertretung durchzuführen ist (vgl. §§ 75 Abs. 3 Nr. 8 und 76 Abs. 2 Nr. 2 BPersVG). Meine Bedenken gegen die Führung dieser Übersichten über Arbeitsergebnisse von Einzelentscheidern sind dem BAFl und dem BMI bereits seit mehr als drei Jahren bekannt (vgl. 16. TB, Nr. 18.9).

Die aus meiner Sicht entscheidende Frage, ob die vom BAFl durch die Übersichten erhobenen Daten für Zwekke der Einsatzplanung, Geschäftsverteilung, Beurteilung, Feststellung der Bewährung sowie die Ausübung der Dienst- und Fachaufsicht erforderlich sind, ist grund-

sätzlich, insbesondere wegen der internen Kenntnisse der Verfahrensabläufe, zum einen zwischen dem BMI, der zuständigen obersten Dienstbehörde als Fachaufsicht, und dem BAFl sowie zum anderen zwischen der zuständigen Personalvertretung und dem BAFl zu regeln. Entsprechendes gilt für die inhaltliche Ausgestaltung der Erhebungsbogen.

Ich hatte das BAFl zunächst gebeten, bis zum Vorliegen der genannten Voraussetzungen auf weitere Erhebungen zu verzichten.

Das BMI hatte ursprünglich die Genehmigung des Verfahrens für den Fall in Aussicht gestellt, daß die Zustimmung der Personalvertretung vorliegt. Diese hat jedoch die Zustimmung zur Einführung des Verfahrens verweigert, so daß weitere Erhebungen zunächst nicht zulässig waren. In dem daraufhin von seiten des BAFl eingeleiteten Stufenverfahren hat auch der Hauptpersonalrat die Zustimmung zur Einführung der Übersichten zunächst mit der Begründung verweigert, daß sie für die genannten Zwecke nicht geeignet seien.

Auf entsprechende Weisung des BMI vom 16. April 1997 hatte das BAFl mit Schreiben vom 13. Mai 1997 schließlich versichert, daß es das Verfahren ausgesetzt und das Mitbestimmungsverfahren eingeleitet habe. Trotz dieser Zusage wurde weiterhin von Enzelentscheidern verlangt, diese Übersichten zu führen. Entsprechende Hinweise wurden von Mitarbeitern des BAFl nunmehr anonym an mich herangetragen, da sie Repressalien von seiten ihrer Vorgesetzten fürchteten.

Daraufhin habe ich das BAFl unter Beteiligung des BMI als oberste Dienstbehörde darum gebeten,

das weitere Führen der Übersichten sofort zu untersagen,

die Ausführung dieser Anweisung zu überprüfen und

mitzuteilen, bei welchen Außenstellen die Übersichten in der vorliegenden Form oder auch in anderer Art und Weise geführt werden.

Hierauf hat das BAFl mitgeteilt, daß es die Führung der Übersicht bis zum Vorliegen der gesetzlichen Voraussetzungen nochmals untersagt habe. Anläßlich einer Prüfung sei festgestellt worden, daß lediglich eine Außenstelle die Übersichten trotz gegenteiliger Weisung weitergeführt hat.

Von einer Dienststelle wurde mir jedoch eine Dienstanweisung zur Weiterführung der Übersichten vorgelegt, die auch der Hauptverwaltung des BAFl bekannt war. Auf diese Dienstanweisung ging das BAFl in seiner oben angegebenen Stellungnahme – obwohl ausdrücklich darauf angesprochen – nicht ein.

Zu meiner Bitte um Auskunft *„auch hinsichtlich aller übrigen Außenstellen“,* beschränkte sich die Antwort darauf, *„daß in einigen Außenstellen die Arbeitsübersichten – zum Teil nur von einigen Einzelentscheidern – freiwillig weitergeführt worden sind“.* In diesem Schreiben wurde mir wiederum versichert, daß *„auch in all diesen Außenstellen mit sofortiger Wirkung die Führung dieser Übersichten untersagt“* worden ist.

Nach § 24 Abs. 4 Satz 1 Nr. 1 BDSG sind die öffentlichen Stellen des Bundes verpflichtet, mir Auskunft zu Fragen zu gewähren, die im Zusammenhang mit meinen datenschutzrechtlichen Kontrollaufgaben nach § 24 Abs. 1 BDSG stehen. Mit Bezug auf diese Vorschrift hatte ich das BAFl konkret um Auskunft gebeten, *„auch hinsichtlich aller übrigen Außenstellen ..., ob die ‚Einzelentscheiderstatistik‘ geführt wird oder seit dem 13. Mai 1997 geführt wurde“.* Die Antwort, *„daß in einigen Außenstellen die Arbeitsübersichten – zum Teil nur von einigen Einzelentscheidern – freiwillig weitergeführt worden sind.“* wurde meiner Frage nicht gerecht. Dem BAFl wäre eine genauere Beantwortung auch möglich gewesen, da es sich um die zusammenfassende Feststellung *„aufgrund einer sofort durchgeführten Umfrage“* handelte. Die Darstellung, daß die *„Arbeitsübersichten ... freiwillig weitergeführt“* worden seien, ist zumindest irreführend. Denn da in mindestens einer Außenstelle die Führung der Übersichten in Kenntnis der Hauptstelle schriftlich angeordnet worden war, erfolgte deren Führung -zumindest durch die dortigen Einzelentscheider – nicht mehr „freiwillig“. Tatsächlich waren Übersichten entgegen klarer Rechts- und Weisungslage in mehreren Außenstellen weitergeführt und an die Hauptverwaltung weitergeleitet worden.

Zu den für meine Entscheidung ausschlaggebenden Gründen, das Verhalten des BAFl wegen mangelnder Unterstützung bei der Erfüllung meiner Aufgaben als einen Verstoß gegen § 24 Abs. 4 BDSG förmlich zu **beanstanden**, zählte auch die Tatsache, daß ich vom BAFl auf meine konkreten Fragen stets ausweichende und zum Teil irreführende Antworten erhalten habe. Im Hinblick auf meine gesetzlichen Kontrollaufgaben muß ich mich jedoch darauf verlassen können, daß auch im schriftlichen Verfahren durch gezielte Fragen eine zweifelsfreie und rückhaltlose Aufklärung datenschutzrechtlich relevanter Sachverhalte erreicht wird.

In seiner Stellungnahme zu der Beanstandung hatte mir der Präsident des BAFl zwischenzeitlich versichert, daß er durch weitere unmißverständliche Weisung sowie durch Kontrollen sowohl der behördlichen Datenschutzbeauftragten als auch der Fachvorgesetzten gewährleiste, daß keine Übersichten mehr geführt werden.

Mit Erlaß vom 18. Januar 1999 hat nunmehr das BMI einer erneuten Einführung mit der Maßgabe zugestimmt, daß

die Übersicht nicht Grundlage einer Beurteilung und eines Zeugnisses sein darf und

die Übersicht auf die Dauer von drei Jahren befristet

geführt werden darf. Der Hauptpersonalrat hat der Maßnahme unter der weiteren Bedingung zugestimmt, daß *„nach Ablauf eines Jahres mit den Personalvertretungen des BAFl sowie dem Hauptpersonalrat die Erfahrungen mit der eingesetzten Statistik beraten werden.“*

Der Fall scheint indes noch nicht abgeschlossen. Nach erneuten Eingaben bestehen Befürchtungen, daß die an sich klaren Vorgaben des BMI in der praktischen Umsetzung umgangen werden und das Steuerungsinstrumentarium letztlich doch wieder als Verhaltens- und Leistungskontrolle genutzt wird.

Ich werde der Sache weiter nachgehen.

18.2.2 Personalfragebögen des BMI – eine Chance für ein ressortübergreifendes einheitliches Verfahren?

Mit der nunmehr eingeführten mehrstufigen Befragung von Bewerbern hat das BMI m.E. ein Verfahren entwikkelt, das ressortübergreifend umgesetzt werden kann.

Bereits mit Inkrafttreten des Neunten Gesetzes zur Änderung dienstrechtlicher Vorschriften zum 1. Januar 1993 wurde vom Gesetzgeber festgelegt, daß ein Dienstherr personenbezogene Daten über Bewerber nur erheben darf, soweit dies zur Begründung und Durchführung des Dienstverhältnisses erforderlich ist. Fragebogen, mit denen diese Daten erhoben werden, bedürfen seit dem 1. Januar 1994 der Genehmigung durch die oberste Dienstbehörde (vgl. § 90 Abs. 4 BBG).

Meine Forderung nach einem zweistufigen Bewerbungsverfahren hat das für das öffentliche Dienstrecht zuständige BMI zwischenzeitlich umgesetzt. In einer ersten Phase werden nunmehr nur Fragen gestellt, die Aussagen zur grundsätzlichen Eignung eines Bewerbers zulassen. Nur die hiernach geeignet erscheinenden Bewerber haben dann in der zweiten Phase eine weitere Gruppe von Fragen zu beantworten, aus denen alle für die endgültige Auswahlentscheidung erforderlichen Informationen hervorgehen (vgl. auch 14. TB Nr. 9.6). Die im Zusammenhang mit der Prüfung der Verfassungstreue erforderlichen Angaben werden mit einer gesonderten Anlage erhoben, die dem sog. Personalbogen II beigefügt ist. Dies entspricht einer von mir erhobenen Forderung (vgl. 13. TB Nr. 2.7.2). Weitere für die Abwicklung des Dienstverhältnisses erforderliche Daten, beispielsweise für die Besoldung oder Beihilfe, werden erst nach Einstellung eines Bewerbers erhoben.

Ich würde es begrüßen, wenn die vom BMI entwickelten Fragebögen Grundlage für ein ressortübergreifendes Konzept werden. Dabei ist mir bewußt, daß die Erforderlichkeit bestimmter Fragen in der ersten Phase eines Bewerbungsverfahrens, abhängig von einer Laufbahn oder bestimmten Funktion, durchaus unterschiedlich sein können. Die hierzu erforderlichen Fragen könnten dann einer Anlage zu dem sog. Personalbogen I angefügt werden. Die vom BMI verwendeten Fragebögen habe ich deshalb – als Muster für den Gebrauch in anderen Bereichen – als **Anlage 26** abgedruckt.

18.2.3 Mitarbeiterbefragung durch den Personalrat zulässig?

Im Zusammenhang mit der grundsätzlichen Einigung über die Einführung einer Gleitzeitregelung sollte sich die Mehrheit der Mitarbeiter der Verwaltung einer obersten Bundesbehörde – vor Abschluß einer entsprechenden Dienstvereinbarung – für die geplante Regelung aussprechen. Hierzu wurde von der Personalvertretung ein Abstimmungsbogen entworfen, in dem die Mitarbeiter durch Ankreuzen erklären konnten, ob sie der Einführung der Gleitzeit zustimmen oder nicht. Der Abstimmungsbogen enthielt außerdem Vor- und Zuname sowie Organisationseinheit, Datum und Unterschrift des Mitarbeiters.

Gegen eine allgemeine Befragung von Mitarbeitern durch die Personalvertretung habe ich keine Bedenken. Im Falle einer personenbezogenen Befragung von Mitarbeitern durch die Personalvertretung halte ich folgendes für wesentlich:

Die Erforderlichkeit der Erhebung personenbezogener Daten (§ 13 Abs. 1 BDSG, § 90 Abs. 4 BBG) kann allgemein nur bejaht werden, wenn der Zweck der Erhebung ohne die erhobenen Daten allgemein nicht erreichbar wäre oder eine Rechtsvorschrift dies erlaubt (vgl. 16. TB Nr. 18.9, 5. Abs.). Ansonsten ist er auf die Freiwilligkeit seiner Angaben hinzuweisen (vgl. § 13 Abs. 3 Satz 2 BDSG).

Instrument der Willensbildung der Personalvertretung ist die Beschlußfassung nach § 37 BPersVG. Zur Vorbereitung ihrer Entscheidung mögen Personalratsmitglieder die an sie in der Sprechstunde herangetragenen Auffassungen der Beschäftigten berücksichtigen – ein allgemeines Recht, nach ihrem Ermessen alle Beschäftigten am Arbeitsplatz aufzusuchen, besteht hingegen nicht. Als dienststelleninternes Ausspracheforum hat das Gesetz das Instrument der Personalversammlung vorgesehen. Dies mag zwar personalvertretungsrechtlich eine allgemeine Befragung durch Fragebogen nicht generell ausschließen; unter dem datenschutzrechtlichen Gesichtspunkt der Erforderlichkeit kommt es allerdings auch darauf an, daß der Erhebungszweck nur bei personenbezogener Durchführung erreicht werden kann.

Auch bei Berücksichtigung dieser Gesichtspunkte ist eine personenbezogene Erhebung durch die Personalvertretung nicht unproblematisch. Denn es kann nicht ausgeschlossen werden, daß die mit dem Bogen namentlich dokumentierte Entscheidung Einfluß auf künftige Entscheidungen des Personalrates in Personalangelegenheiten hat.

Aufgrund dieser allgemeinen Hinweise und meinen auf die Besonderheiten des Einzelfalls bezogenen Empfehlungen haben Dienststelle und Personalvertretung im einvernehmlichen Zusammenwirken mit dem internen Datenschutzbeauftragten eine datenschutzrechtlich akzeptable Lösung gefunden. Dabei wurden die ausgefüllten Fragebogen dem internen Datenschutzbeauftragten übergeben, von diesem anonymisiert und ausgewertet. Dem Personalrat wurde lediglich das Ergebnis der Auswertung zur Verfügung gestellt. Die Fragebogen wurden vom internen Datenschutzbeauftragten vernichtet.

18.2.4 Datenerhebung bei Rückforderung überzahlter Bezüge

Ein Versorgungsempfänger aus dem Geschäftsbereich des BMVg wandte sich hilfesuchend an mich, nachdem überzahlte Bezüge in Höhe von etwa 2 500 DM von ihm zurückgefordert worden waren.

Auf seine Bitte, den Betrag in zehn Raten von je 250 DM zurückzahlen zu können, wurde er aufgefordert, ein Formular „Erklärung über die wirtschaftlichen Verhältnisse“ auszufüllen. In dem Formular wurde eine umfassende, höchst detaillierte Auskunft nicht nur zu ihm selbst, sondern teilweise auch zu seiner Ehefrau verlangt.

So sollten die monatlichen Nettoeinkünfte, aufgeschlüsselt nach elf verschiedenen Einkunftsarten, genau angegeben werden. Zudem war nach dem Verkehrswert etwaigen Immobilienbesitzes, Sparguthaben, Wertpapieren, Bargeld und anderen Wertgegenständen gefragt. In einer weiteren Rubrik sollten – unter Beifügung von Belegen – die monatlichen Verpflichtungen genau aufgeschlüsselt werden bis hin zu den Kosten für Beleuchtung und Heizung. Das BMVg hat mir mitgeteilt, daß die Verwendung des Formulars in seinem Geschäftsbereich nicht vorgeschrieben sei. Vielmehr würden im allgemeinen die zur Rückzahlung Verpflichteten ohne detaillierte Fragestellung in einem Schreiben aufgefordert, ihre finanziellen Verhältnisse eingehend darzulegen. Das führe allerdings letzten Endes zum gleichen Ergebnis.

Die Forderung nach einer so weitgehenden Offenlegung der wirtschaftlichen Verhältnisse ist unverhältnismäßig, wenn es um einen vergleichsweise geringen Rückforderungsbetrag geht, der die Höhe des Betrages von einem oder zwei Monatsbezügen des Betroffenen nicht überschreitet. Das BMVg hat mir zugesagt, die betroffenen Dienststellen zu bitten, zukünftig von einer detaillierten Erhebung von Angaben über die wirtschaftlichen Verhältnisse abzusehen, wenn es sich um vergleichsweise geringe Rückforderungsbeträge handelt.

18.2.5 Laxer Umgang mit Personalaktendaten bei der Bundesanstalt für Arbeit beanstandet

Zur Aufklärung des Sachverhalts um die fristgerechte Abgabe einer Arbeitsunfähigkeitsbescheinigung eines Mitarbeiters hatte ein Arbeitsamt in Niedersachsen umfangreiche Informationen über einen Mitarbeiter eines Arbeitsamtes in Nordrhein-Westfalen gesammelt, der vom Betroffenen als Zeuge für eine fristgerechte Abgabe der Bescheinigung benannt war.

Gegen eine im Zusammenhang mit der Abmahnung des Mitarbeiters des Arbeitsamtes in Niedersachsen vorgenommene Befragung seines Kollegen beim Arbeitsamt in Nordrhein-Westfalen durch die dortige Personalstelle habe ich im Grundsatz keine Bedenken, soweit die Erhebung der Daten zur Aufklärung des Sachverhalts hinsichtlich der Abgabe der Arbeitsunfähigkeitsbescheinigung, die zur Abmahnung führte, erforderlich gewesen wäre. Die vom Arbeitsamt in Niedersachsen über das Arbeitsamt in Nordrhein-Westfalen an den dortigen Mitarbeiter gerichteten Fragen waren zum größten Teil jedoch nicht erforderlich, um in Erfahrung zu bringen, ob die in Rede stehende Arbeitsunfähigkeitsbescheinigung fristgerecht eingegangen war. Die Erforderlichkeit der umfangreichen Befragung des Mitarbeiters des Arbeitsamtes in Nordrhein-Westfalen hätte nur bejaht werden können, wenn der Erhebungszweck – die Überprüfung des fristgerechten Eingangs der Arbeitsunfähigkeitsbescheinigung des Mitarbeiters des Arbeitsamtes in Niedersachsen ohne sie allgemein nicht möglich gewesen wäre (vgl. § 90 Abs. 4 BBG). Die Bundesanstalt für Arbeit hat dazu eingeräumt, daß *„ein so intensiver und umfangreicher Datenaustausch zwischen den Arbeitsämtern nicht notwendig gewesen wäre“.*

Der Zugang zu Personalaktendaten ist auf Zwecke der Personalverwaltung und Personalwirtschaft beschränkt (vgl. § 90 Abs. 1 Satz 3 und Abs. 3 BBG). Ein Austausch von Personalaktendaten, die den beruflichen Werdegang der jeweiligen Mitarbeiter betreffen, war zur Aufklärung des Sachverhalts um die Abgabe der Arbeitsunfähigkeitsbescheinigung nicht erforderlich. Der umfangreiche Austausch von Personalaktendaten zwischen den Arbeitsämtern ging über das zur Sachaufklärung erforderliche Maß hinaus und stellt damit einen Verstoß gegen das Personalaktengeheimnis dar, den ich gemäß § 25 BDSG **beanstandet** habe.

Aber auch die Ablage des in dieser Angelegenheit entstandenen Schriftverkehrs, die nach den mir vorliegenden Unterlagen in der jeweiligen Personalhauptakte der Mitarbeiter erfolgte, ist datenschutzrechtlich unzulässig, selbst dann, wenn die Bundesanstalt für Arbeit erklärt, daß dies so in ihrer Personalaktenrichtlinie vom 18. April 1989 geregelt ist. Danach sind für Vorgänge von geringer oder nur vorübergehender Bedeutung „Personal-Beiakten“ anzulegen und fortlaufend zu numerieren.

Mit Inkrafttreten des Neunten Gesetzes zur Änderung dienstrechtlicher Vorschriften zum 1. Januar 1993 entspricht die genannte Richtlinie nicht den gesetzlichen Vorgaben der §§ 90ff. BBG. Die Erarbeitung entsprechender Regelungen für die Bundesanstalt für Arbeit wurde mir seit Jahren zugesichert. Nach der aktuellen Gesetzgebung gehören zur Personalakte alle Unterlagen, die den Beamten betreffen, soweit sie mit seinem Dienstverhältnis in einem unmittelbaren inneren Zusammenhang stehen (Personalaktendaten); andere Unterlagen dürfen in die Personalakte nicht aufgenommen werden (vgl. § 90 Abs. 1 Satz 2 BBG).

Da Daten in den Personalakten der jeweiligen Mitarbeiter – wie oben ausgeführt – zum überwiegenden Teil unzulässigerweise ausgetauscht wurden und durch die Ablage des genannten Schriftverkehrs in den Personalakten jeweils auch Personaldaten Dritter aufgenommen wurden, was ebenfalls nicht in Einklang mit den gesetzlichen Vorgaben des § 90 Abs. 1 BBG steht, habe ich die Bundesanstalt für Arbeit gebeten, diese Daten umgehend zu löschen. Außerdem habe ich die Personalaktenführung der beiden Mitarbeiter gemäß § 25 BDSG als einen Verstoß gegen die gesetzlichen Vorgaben zur Personalaktenführung beanstandet. Darüber hinaus habe ich gebeten, die offenbar noch angewandten Personalaktenrichtlinien vom 18. März 1989 außer Kraft zu setzen. Die Bundesanstalt für Arbeit hat mir zwischenzeitlich den Entwurf der Neufassung einer Personalaktenrichtlinie vorgelegt.

18.3 Verarbeitung und Nutzung von Personaldaten der Mitarbeiter

18.3.1 Veröffentlichung von Personaldaten Hausmitteilungen – immer wieder Gegenstand von Eingaben

Gegen eine Veröffentlichung offenkundiger Daten, wie Name, Dienstzimmer, Nebenstellennummer, Funktions-

übertragung, längerfristige Beurlaubung in **Hausmitteilungen** habe ich mich zu keiner Zeit ausgesprochen. Daß derartige Angaben behördenintern allgemein bekannt gemacht werden, entspricht einem unabweisbaren dienstlichen Bedürfnis. Das gilt beispielsweise auch für die Amtsbezeichnung der Beamten, deren Führung zu den hergebrachten Grundsätzen des Berufsbeamtentums zu rechnen ist; auch wenn aus der Amtsbezeichnung die Besoldungsgruppe abgeleitet werden kann.

Es ist jedoch erforderlich, zwischen einfachen Mitteilungen, wie z. B. Funktionsübertragungen, Einstellungen, Abordnungen, Versetzungen und solchen, die zusätzliche Informationen geben, wie z. B. Beurlaubung wegen Mutterschutz, Erziehungsurlaub, Beurlaubung für eine Verwendung bei der XYZ BT-Fraktion oder Namensänderung aufgrund Ehescheidung, zu differenzieren. Diese Daten, die den Grund von Personalmaßnahmen nennen und damit Rückschlüsse auf persönliche, private Verhältnisse von Mitarbeitern zulassen, sind anders zu behandeln. In Abstimmung mit dem BMI konnte ich insoweit bereits 1986 erreichen, *„daß Wünschen von Bediensteten, auf die Bekanntgabe ihrer Daten in den Hausmitteilungen zu verzichten, ausnahmslos nachgekommen“* wird (vgl. 9. TB Nr. 7.1.4 letzter Anstrich).

Mit Inkrafttreten des Neunten Gesetzes zur Änderung dienstlicher Vorschriften wurde dieser Praxis Rechnung getragen. Das Gesetz verdeutlicht in den §§ 90ff. BBG, daß die betroffenen Mitarbeiter stärker in den Umgang mit ihren Personalaktendaten einbezogen werden sollen.

Sicher sind an die Veröffentlichung in Hausmitteilungen nicht die hohen Anforderungen einer Übermittlung an Dritte im Sinne des § 90d Abs. 2 BBG zu stellen, da es sich bei einer Weitergabe innerhalb einer speichernden Stelle lediglich um eine Nutzung, nicht jedoch um eine Übermittlung an eine andere speichernde Stelle handelt. Dennoch ist auch hier der Wille der Betroffenen bei der Veröffentlichung zu berücksichtigen. Ich halte es für notwendig, die Mitarbeiter darüber zu informieren, daß sie der Veröffentlichung widersprechen können. Diese Vorgabe werde ich weiterverfolgen.

Zum Thema „Hausmitteilungen“ haben mir die Landesbeauftragten für den Datenschutz mitgeteilt, daß auch in ihren Zuständigkeitsbereichen eine zunehmende Sensibilität hierzu besteht, die sich in einer restriktiveren Veröffentlichungspraxis niederschlägt.

Im Interesse eines guten Arbeitsklimas empfehle ich allen Stellen, die Hausmitteilungen herausgeben, in Zweifelsfällen die Wünsche der Mitarbeiter zu berücksichtigen.

18.3.2 Privatanschriften bei Gehalts-/Bezügemitteilungen

Die Gehalts-/Bezügemitteilungen für die Beschäftigten der Bundesbehörden werden vom BfF erstellt und in Fensterbriefumschlägen kuvertiert und an die Beschäftigungsdienststellen zur Verteilung gegeben. Infolge einer Verfahrensumstellung, u. a. zur rationelleren Zustellung an die Versorgungsempfänger wird seit Anfang 1998 neben dem Namen, der Dienststellennummer und der Kennummer auch die Privatanschrift des Empfängers gedruckt. Üblicherweise erhalten die Bediensteten ihre Gehalts-/Bezügemitteilungen unmittelbar von dem behördlichen Boten. Diese und andere Bedienstete, z. B. der Vertreter des Empfängers können dann die Privatanschrift des Empfängers erfahren. Einige Bedienstete haben sich daraufhin an mich gewandt. Vor allem Frauen legten Wert darauf, daß ihre Privatanschrift im Kollegenkreis gar nicht oder nur mit ihrer Einwilligung bekannt wird.

Ich teile die Bedenken der Bediensteten. Das BMF hat mir als Lösung vorgeschlagen, daß die Beschäftigungsdienststelle als anordnende Stelle dem BfF statt der Privatanschrift die Anschrift der Dienststelle zur Speicherung im Zahlungsbestand meldet. Auf meine ergänzende Empfehlung hin werden die Beschäftigten bei den anordnenden Stellen auf diese Möglichkeit in allgemeiner Form hingewiesen. Hierdurch wird sichergestellt, daß die mit dem Andruck der Privatanschrift im Adressfeld verbundenen Vorteile erhalten bleiben. Sie verringert das Risiko der Verwechslung der Gehalts-/Bezügemitteilungen namensgleicher Empfänger innerhalb einer Beschäftigungsdienststelle – einem ebenfalls datenschutzrechtlichen Problem, das in der Vergangenheit aufgetreten war.

18.3.3 Wieviel Schutz brauchen Vor- und Nachname wirklich?

Ob und in welchem Umfang sich Amtsträger auf das Recht auf informationelle Selbstbestimmung berufen können, wenn es darum geht, bei ihrem dienstlichen Auftreten gegenüber Bürgern ihre Identität preiszugeben, wird immer wieder grundsätzlich und kontrovers diskutiert. Folgende Fallkonstellationen waren im Berichtszeitraum zu bewerten:

- Zugbegleiter der Deutschen Bahn AG sind von ihrer vorgesetzten Stelle angewiesen, dem Kunden auf Verlangen Namen, Amtsbezeichnung und Dienststelle anzugeben;
- Zollbeamte haben nach internen Regelungen Reisenden grundsätzlich ihren Namen sowie ihre Dienststelle zu nennen oder sich auszuweisen und zwar auch, wenn sie in Dienstkleidung auftreten;
- um ratsuchenden Bürgern nicht als anonymer Verwaltungsapparat zu erscheinen, und um der Transparenz der öffentlichen Verwaltung Rechnung zu tragen, wird in Antwortschreiben der BfA stets der Name des zuständigen Mitarbeiters genannt;
- Bei der BKK POST wurden Mitarbeiter, die Kontakt zu Versicherten aufnehmen, zur Nennung von Vor- und Nachnamen verpflichtet.

Die allgemeine Einstellung zu Namensnennung und Anrede befindet sich im Umbruch. Daß auch der Vorname nicht mehr der rein private Bestandteil des Namens ist, entspricht einer veränderten, allgemeinen Einstellung gegenüber traditionellen Vorstellungen. So ist es heute praktisch ausnahmslos üblich, daß sich z. B. Mitarbeiter von Call-Centern oder anderen telefonisch angebotenen Dienstleistungen mit Vor- und Nachnamen melden. In

der Presse werden Personen regelmäßig mit Vor- und Nachname genannt und Visitenkarten enthalten gewöhnlich nicht nur Vor- und Nachname, sondern weitere Angaben zur Person.

Auch wegen dieser veränderten Einstellung habe ich gegen eine Verpflichtung von Mitarbeitern, ihren Vor- und Nachnamen zu nennen, grundsätzlich keine Bedenken, vor allem, wenn sie – wie bei BfA oder BKK Post – einen engen, auf Service orientierten Kontakt zum Bürger haben (siehe auch 16. TB Nr. 33.1).

Die Frage des Rechts auf informationelle Selbstbestimmung für Amtsträger, wie z. B. Zollbeamte, ist von mir auch mit den Kollegen in den Bundesländern erörtert worden. Im Mittelpunkt stand dabei die Frage, ob sich ein Amtsträger – als handelndes Organ des Staates – überhaupt auf das informationelle Selbstbestimmungsrecht berufen kann.

Nach meiner Auffassung kann sich ein Beamter gegenüber dem Staat auf sein informationelles Selbstbestimmungsrecht nur in seiner Eigenschaft als eigenständiger Träger von Rechten und Pflichten berufen. Dies ist beispielsweise der Fall, wenn bei Beamten das sogenannte Grundverhältnis zu seinem Dienstherrn berührt wird, indem der Dienstherr personenbezogene Daten des Beamten für Zwecke der Personalverwaltung oder Personalwirtschaft erhebt, verarbeitet oder nutzt (s. o. Nr. 18.2.2).

Soweit ein Beamter dagegen als Amtsträger für den Staat handelt, dem diese Tätigkeit zugerechnet wird, ist sein informationelles Selbstbestimmungsrecht jedoch stark eingeschränkt. Deshalb hat ein Beamter beispielsweise kein Verfügungsrecht darüber, ob sein Name in den von ihm bearbeiteten Vorgängen, in dienstlichen Telefonverzeichnissen oder im Geschäftsverteilungsplan erscheint. Die Angabe des Namens etc. von Zugbegleitung und Zollbeamten gegenüber Reisenden im Zusammenhang mit ihren Dienstaufgaben beeinträchtigt insoweit deren informationelles Selbstbestimmungsrecht nicht.

Dies schließt aber nicht aus, daß in bestimmten Einzelfällen eine besondere Rücksichtnahme gegenüber einzelnen Mitarbeitern geboten ist. Einschränkungen bei der Verarbeitung und Nutzung von Beschäftigtendaten, die nicht das Grundverhältnis betreffen, ergeben sich im Einzelfall aus den hergebrachten Grundsätzen des Berufsbeamtentums und aus beamtenrechtlichen Regelungen – vor allem der Fürsorgepflicht. So darf beispielsweise ein Beamter des Zolls oder der Bahn die Angabe seines Namens verweigern, wenn nach den Umständen des Einzelfalles zu befürchten ist, daß ansonsten seine persönliche Sicherheit oder der Erfolg der Amtshandlung gefährdet würde.

18.3.4 „Wess' Brot ich eß'......" – Nutzung von Personaldaten zu Werbezwecken

„Der Bäckergeselle würde Brötchen auch bei seinem Meister kaufen – oder?"

Mit dieser Aufforderung wurden die Beschäftigten einer Niederlassung der Deutschen Post AG, die bislang ihr Gehaltskonto nicht bei der POSTBANK geführt hatten, von ihrem Niederlassungsleiter persönlich an eine zuvor bereits schriftlich geäußerte Bitte erinnert, mit ihrem Gehaltskonto künftig zum ehemaligem Kooperationspartner der Deutschen Post AG der jetzigen Tochtergesellschaft zu wechseln. Für die Anschreiben des Niederlassungsleiters wurden Daten aus der Personalabteilung verwendet, die ausschließlich für den Zweck der Bezügeüberweisung erhoben und gespeichert worden waren.

Diese „Werbeschreiben" waren für mich Anlaß, die Nutzung von Mitarbeiterdaten für Werbezwecke mit der Generaldirektion der Deutschen Post AG grundsätzlich zu erörtern.

Personalaktendaten, dazu gehören auch die Bankverbindungen der Mitarbeiter für die Überweisung der Bezüge- und Gehaltszahlungen, dürfen grundsätzlich nur

a) im Rahmen der Zweckbestimmung eines Vertragsverhältnisses oder eines vertragsähnlichen Vertrauensverhältnisses mit dem Betroffenen,
b) soweit es zur Wahrung berechtigter Interessen der speichernden Stelle erforderlich ist und kein Grund zu der Annahme besteht, daß das schutzwürdige Interesse des Betroffenen an dem Ausschluß der Verarbeitung oder Nutzung überwiegt,

als Mittel für die Erfüllung eigener Geschäftszwecke genutzt werden (vgl. § 12 Abs. 4 i.V.m. § 28 Abs. 1 Nr. 1 und 2 BDSG).

Diese Regelung beschränkt den Zugang zur Personalakte zunächst auf Beschäftigte, die im Rahmen der Personalverwaltung mit der Bearbeitung von Personalangelegenheiten betraut sind. Die abschließend aufgezählten Ausnahmen stehen unter dem Vorbehalt schutzwürdiger Interessen der Betroffenen. Beide Schreiben wurden vom Niederlassungsleiter unterschrieben; der Grund für die Schreiben, daß die angeschriebenen Mitarbeiter ihr Gehaltskonto nicht bei der POSTBANK führen, wurde der Personalakte (Besoldungsakte) der Mitarbeiter entnommen.

Die Personalaktendaten der betroffenen Mitarbeiter wurden vom Dienstvorgesetzten, der auch für Personalentscheidungen zuständig ist, unzulässig genutzt. Es kann auch nicht ausgeschlossen werden, daß im vorliegenden Fall die „Werbung" der Mitarbeiter für die POSTBANK sowie die entsprechende Erfolgskontrolle Auswirkungen auf künftige Personalentscheidungen hat. Das schutzwürdige Interesse der betroffenen Mitarbeiter am Ausschluß der Nutzung ihrer Personalaktendaten zu Werbezwecken ist aus meiner Sicht höher einzustufen als das durchaus berechtigte Interesse des Betriebes an der Erfüllung eigener Geschäftszwecke der POSTBANK. Die Nutzung der Bankverbindungsdaten aus den Besoldungsakten der Mitarbeiter für Werbezwecke verstößt gegen § 12 Abs. 4 i.V.m. § 28 Abs. 1 BDSG.

Zu sehen ist in diesem Zusammenhang die wesentlich stringentere Zweckbindung der Personalaktendaten von Beamten nach dem Bundesbeamtengesetz, das eine Verwendung für Zwecke außerhalb der Personalverwaltung und Personalwirtschaft von der Einwilligung des Beamten abhängig macht (vgl. § 90 Abs. 1 Satz 3 BBG).

Auf eine Beanstandung gemäß § 25 BDSG gegenüber der Deutschen Post AG habe ich verzichtet, weil mir versichert wurde, daß

1. künftig keine Personaldaten in der genannten Art und Weise zu Werbezwecken verwendet werden,
2. den von der Werbemaßnahme betroffenen Mitarbeitern das Bedauern hinsichtlich der Verletzung datenschutzrechtlicher Bestimmungen ausgedrückt wird und
3. die aus der genannten Werbeaktion gewonnenen Daten gelöscht wurden.

18.3.5 Personaldaten beim Referatsleiter

In einer Bundesbehörde hatte ein Referatsleiter seinen Mitarbeitern sog. blaue Briefe geschrieben, in denen er allgemein ihre fachlichen Leistungen kritisierte und sie aufforderte, ihre Dienstpflichten zukünftig gewissenhafter wahrzunehmen. Die Schreiben trugen Aktenzeichen „...- Pers. <Name des Mitarbeiters>“. Die Entwürfe der Schreiben verwahrte der Referatsleiter bei sich.

Die Führung von Vorgängen zu jedem Mitarbeiter ist eine ausschließliche Aufgabe der Personalverwaltung. Sie sind bei der Personalstelle zu verwahren. Ihre Aufbewahrung im Fachreferat bedeutet eine Führung unzulässiger Nebenakten. Die Erstellung des eingangs beschriebenen Schreibens durch den Leiter des Fachreferats und seine Aufbewahrung im Fachreferat habe ich daher als datenschutzrechtlich unzulässig bewertet. Zwar gehört zur allgemeinen Personalführung durch den Leiter des Fachreferats auch die Einzelaufgaben übergreifende mitarbeiterbezogene Motivation, beispielsweise durch Äußerungen im regelmäßigen Arbeitskontakt oder durch Personalführungsgespräche. Ein Vorgehen, das darauf zielt, Fakten zulasten eines Mitarbeiters zu dokumentieren und zu sammeln, ist nach seiner Zweckbestimmung dagegen wenigstens mittelbar bereits auf eine Personalmaßnahme gerichtet und somit als deren Aufgabe der Personalstelle selbst vorbehalten. Derartige Vorgänge sind bei der Personalstelle zu führen.

Personenbezogene Notizen des Leiters von Fachreferaten halte ich nur für zulässig, soweit sie für die organisatorische und personelle Führung des Referats erforderlich sind. Ebenfalls im Hinblick auf die Steuerung der Aufgabenerledigung kann sich der Referatsleiter erteilte Arbeitsaufträge und terminliche Vorgaben notieren. Notizen dieser Art sind zu vernichten, sobald sie für die Aufgabensteuerung durch den Referatsleiter nicht mehr benötigt werden. Das ist regelmäßig dann der Fall, wenn die Maßnahmen oder Zeiträume, auf die sie sich beziehen, abgeschlossen sind.

Notizen des Referatsleiters im Hinblick auf die künftige Beurteilung oder ihre potentielle Bedeutung für Personalmaßnahmen gegenüber einzelnen Mitarbeitern halte ich nur innerhalb sehr enger Grenzen für zulässig, nämlich insoweit, als dies dafür zur Gedächtnisstütze über Sachverhalte (objektive Tatsachen, Fakten) erforderlich ist. Ihrem Charakter als persönliche Gedächtnisstütze entsprechend kann deren Weitergabe an einen Funktionsnachfolger des Referatsleiters nicht in Betracht kommen. Soweit eine Beurteilung auch den vor dem Vorgesetztenwechsel liegenden Zeitraum umfassen soll, muß der frühere Vorgesetzte für diese Zeit eine eigene Beurteilung abgeben oder zumindest einen Beurteilungsbeitrag liefern.

Das Personalführungsgespräch ist ein Instrument kooperativer Führung; es dient der Motivation und Förderung des Mitarbeiters. Die Notwendigkeit, ein Protokoll oder einen Vermerk über das Gespräch anzufertigen, hängt im wesentlichen von seinem Inhalt und den getroffenen Feststellungen ab. Protokoll oder Vermerk dienen der Personalverwaltung und sind daher bei der Personalstelle aufzubewahren. Der Betroffene sollte seine Kenntnisnahme dokumentieren. Dies schließt die Möglichkeit zu einer Gegendarstellung ein.

18.4 Personaldaten im Intranet des Bundes

Der Ausbau des Informationsverbundes Berlin-Bonn – IVBB – zum Intranet der Bundesverwaltung schreitet weiter voran. Angeschlossen an dieses „Internet der Bundesverwaltung“ sind ausschließlich Bundesbehörden. Der Umgang mit dem neuen Medium gestaltet sich zum Teil schwierig, auch weil noch eine gewisse Unsicherheit besteht, welche personenbezogenen Daten der Mitarbeiter der angeschlossenen Behörden in das Intranet eingestellt werden dürfen. Irritationen entstanden beispielsweise bei der Frage der Veröffentlichung von internen Telefonverzeichnissen oder Stellenausschreibungen. Ich habe das zum Anlaß genommen, im Rahmen von Beratungen hierzu grundsätzlich Stellung zu nehmen.

Gegen die Bereitstellung von dienstlichen Telefonverzeichnissen im IVBB-Intranet – zu dem ausschließlich Bundesbehörden Zugang haben – bestehen keine Bedenken. Entsprechendes gilt für Stellenausschreibungen, da sie keine personenbezogenen Daten enthalten.

Allgemein kann als Richtschnur gelten, daß durch die Nutzung des Intranet datenschutzrechtliche Standards entsprechender konventioneller Verfahren nicht unterschritten werden dürfen. So kann für interne Telefonverzeichnisse im IVBB genauso wenig wie für die gedruckten dienstlichen Telefonverzeichnisse eine absolute Garantie gegeben werden, daß sie nicht vorschriftswidrig an Stellen außerhalb der Bundesverwaltung gelangen.

Eine generelle Aussage, nach der die Bereitstellung von personenbezogenen Daten oder speziell Personaldaten zum Abruf im IVBB-Intranet unbedenklich sei, wäre allerdings zu weitgehend. Für Personaldaten gelten die Bestimmungen der §§ 90ff. BBG. Diese Vorschriften enthalten auch Vorgaben für deren automatisierte Verarbeitung. Beispielsweise dürfen Personalaktendaten *„automatisiert nur im Rahmen ihrer Zweckbestimmung und nur von den übrigen Personaldaten technisch und organisatorisch getrennt verarbeitet und genutzt werden.“* (§ 90g Abs. 2 BBG). Nach § 90g Abs. 1 Satz 3 BBG ist ein automatisierter Datenabruf durch andere Behörden unzulässig, soweit durch besondere Rechtsvorschrift nichts anderes bestimmt ist. Grundsätzlich sollte vor der Bereitstellung von Personaldaten (nicht

nur: Personal**akten**daten) im IVBB-Intranet **zum Abruf** auch jenseits zwingender gesetzlicher Grenzen Zurückhaltung gelten, und zwar selbst dann, wenn dies nur einer geschlossenen Benutzergruppe zugänglich ist.

Gegen die Übermittlung von Personaldaten als E-Mail im Intranet zwischen Stellen, zwischen denen diese Daten auf konventionellen Wegen befugt übermittelt werden dürften, habe ich entsprechend der oben genannten Richtschnur keine grundsätzlichen Bedenken, wenn ein dem zulässigen konventionellen Übermittlungsweg entsprechender Sicherheitsstandard im Intranet gewährleistet ist. Vorbehaltlich einer näheren Prüfung könnte beispielsweise in einer Ende-zu-Ende-verschlüsselten E-Mail im IVBB-Intranet eine datenschutzrechtlich hinreichende Entsprechung zu einer konventionellen Verschlußmappe zu sehen sein (siehe hierzu auch Nr. 8.6).

Solange die Nutzung des IVBB-Intranet (noch) nicht zu einem von allen Bediensteten beherrschten Arbeitsmittel geworden ist, halte ich unter Transparenzgesichtspunkten eine wenigstens allgemeine Information aller Bediensteten über die im Intranet bereitgehaltenen personenbezogenen Daten für erforderlich.

Soweit Personaldaten – z. B. in einem Telefonverzeichnis – im IVBB-Intranet zum Abruf bereitgestellt werden, liegt datenschutzrechtlich die Verantwortlichkeit bei der Stelle, die die Personaldaten eingestellt hat. Sie ist für die **Richtigkeit** und damit auch für die stete **Aktualität** verantwortlich. Bei einer Verbreiterung des personenbezogenen Angebots im IVBB muß daher auch aus datenschutzrechtlichen Gründen die erforderliche Personalkapazität zur Pflege der Daten bereitstehen. Für die Pflege der Daten auf jedem Server einer angeschlossenen Stelle sollte eine Person dieser Stelle verantwortlich sein. Bei jedem IVBB-Intranet-Angebot mit personenbezogenen Daten sollte diese Person und ihre Erreichbarkeit angegeben werden, damit betroffene Bedienstete eventuelle Berichtigungshinweise geben bzw. -ansprüche geltend machen können.

Diese Empfehlungen gehen von einem Ausbauzustand des IVBB-Intranet aus, bei dem der Anschluß auf Bundesbehörden beschränkt ist. Für den Fall einer mittel- oder langfristigen Öffnung auch für Landesbehörden oder andere Stellen wäre eine neue Bewertung erforderlich.

18.5 Umfang und Grenzen des Schutzes von Beihilfe

§ 90a BBG stellt Beihilfedaten unter einen ganz besonderen Schutz. Nur innerhalb enger Grenzen ist eine Offenbarung von Beihilfedaten zulässig. Mit diesen engen Voraussetzungen will der Gesetzgeber der besonderen Schutzbedürftigkeit von Beihilfedaten Rechnung tragen.

Um Beihilfeleistungen zu bekommen, hat der Beamte Daten über seinen Gesundheitszustand weiterzugeben, die keinen unmittelbaren Bezug zum Dienstverhältnis haben und die vom Fragerecht des Arbeitgebers nicht erfaßt wären. Er kann dem auch nicht durch Verzicht auf Beihilfe ausweichen, wenn er wirtschaftlich auf die Beihilfeleistungen angewiesen ist.

Eine Konsequenz hieraus ist die Abschottung der Beihilfestelle von der übrigen Personalverwaltung und die hohe gesetzliche Schwelle für eine Offenbarung von Beihilfedaten. Die medizinischen Daten, die im Rahmen des Beihilfeverfahrens anfallen, würden der Dienststelle bei einem Angestellten oder Arbeiter überhaupt nicht bekannt werden. Ein Beamter und seine Angehörigen müssen sich also darauf verlassen können, daß Beihilfedaten nicht auch für andere Zwecke verwendet werden. Gerade bei ärztlichen Leistungen, die vorab genehmigt werden müssen, wie z. B. Psychotherapien, zeigt sich, wie wichtig der Schutz des Beihilfeverfahrens ist. Hier sind die Betroffenen besonders stark emotional beteiligt, haben leichter Angst, daß ihre Krankheit bekannt wird, und die Beihilfestellen müssen wissen, daß das Gesetz ihr Schweigen, z. B. gegenüber den Dienstvorgesetzten, grundsätzlich rechtfertigt. Dennoch ergeben sich hier immer wieder Fragen, die oft auch an mich herangetragen werden.

18.5.1 Grenzen der Zweckbindung von Beihilfedaten und der ärztlichen Schweigepflicht

Nach § 90a Satz 4 BBG dürfen Beihilfedaten, also medizinische Daten eines Beamten, ohne seine Einwilligung nur offenbart werden zur Abwehr

– erheblicher Nachteile für das Gemeinwohl,
– einer sonst unmittelbar drohenden Gefahr für die öffentliche Sicherheit oder
– einer schwerwiegenden Beeinträchtigung der Rechte einer anderen Person.

Diesen Ausnahmetatbeständen dürfte in der Praxis zurecht nur äußerst geringe Bedeutung zukommen. Gleichwohl hatten sich im Berichtszeitraum eine Dienststelle und ihr Personalrat an mich gewandt, um sich zu einem Fall beraten zu lassen, der unter diese Ausnahmen hätte fallen können. Es handelte sich um einen sicherheitsüberprüften Beamten, der sich bei der Beihilfestelle über die Erstattungsfähigkeit einer Alkohol-Entwöhnungskur erkundigt hatte.

Die Anwendung der Ausnahmen nach § 90a Satz 4 BBG fordert eine sorgfältige Abwägung zwischen dem Gemeinwohl und dem informationellen Selbstbestimmungsrecht des Beihilfeberechtigten. So kann der Gemeinwohlvorbehalt in § 90a Satz 4 BBG es rechtfertigen, personenbezogene Daten, die bei der Beihilfestelle gespeichert sind, an andere Stellen weiterzugeben, wenn dies für Maßnahmen nach dem Sicherheitsüberprüfungsgesetz erforderlich ist. Bei dieser Interessenabwägung sind auch das Verhältnismäßigkeitsgebot und das Übermaßverbot zu beachten.

Im vorliegenden Fall habe ich insbesondere noch auf folgende Gesichtspunkte hingewiesen:

– Die Weitergabe der Daten durch den Betroffenen selbst, z. B. im Rahmen eines Gespräches mit der Beihilfestelle oder mit seiner Einwilligung (§ 90a Satz 4, 1. Alternative BBG), ist jedenfalls die im Sinne des Übermaßverbots weniger einschneidende Maßnahme und daher vorzuziehen. Dieser Weg hätte

sich im vorstehenden Fall besonders empfohlen, da der Betroffene durch seine Frage nach einer Alkohol-Entwöhnungskur Problembewußtsein bewiesen hatte. Grundsätzlich sollte zunächst der Betroffene von der Beihilfestelle darauf hingewiesen werden, selbst die Stelle zu informieren, an die die Beihilfestelle möglicherweise Daten weiterzugeben beabsichtigt.

– Dürfen Beihilfedaten ausnahmsweise weitergegeben werden, sollte der Betroffene wegen des Transparenzgebotes und wegen der Fürsorgepflicht grundsätzlich darüber unterrichtet werden. Dies hebt auch bereits die amtliche Begründung zu § 90a BBG (BT-Drs. 12/544) hervor.
– Sorgfältig zu entscheiden ist auch, an wen die Daten weitergegeben werden. Sind mögliche Sicherheitsrisiken in der Person des Beamten der Grund für die Weitergabe, kommt diese, wenn überhaupt, grundsätzlich nur an den Geheimschutzbeauftragten und nicht an die Personalstelle in Betracht. Die Aufgaben der zuständigen Stelle – hier des Geheimschutzes nach dem SÜG – sind nämlich gemäß § 3 Abs. 1 Satz 3 SÜG von der Personalverwaltung getrennt wahrzunehmen. Kommt diese Stelle – nach Prüfung der Sicherheitserheblichkeit der Erkenntnisse – zu dem Ergebnis, daß dem Betroffenen der Sicherheitsbescheid entzogen wird, unterrichtet sie die Personalstelle nur hierüber. Die medizinischen Daten dürfen dabei nicht weitergegeben werden.

Im Ausgangsfall kamen diese Überlegungen leider nicht mehr zum Zuge, da die Beihilfestelle die problematisierten Daten an die Personalverwaltung bereits weitergeleitet hatte.

18.5.2 Organisatorische Eingliederung der Beihilfestelle verbesserungsbedürftig

Der interne Datenschutzbeauftragte sowie der Personalrat beim Deutschen Patentamt hatten datenschutzrechtliche Bedenken hinsichtlich der Abschottung der Beihilfestelle im Sinne des § 90a BBG vorgetragen und mich um Beratung gebeten.

Anläßlich eines Beratungsgespräches vor Ort stellte ich fest, daß das Sachgebiet, in dem u. a. Beihilfeangelegenheiten bearbeitet werden, einem Referat angegliedert ist, dessen Referatsleiter auch für Personalangelegenheiten der Angestellten und Lohnempfänger zuständig ist. Aus dem Geschäftsverteilungsplan war nicht ersichtlich, daß er nicht auch die Fachaufsicht in Beihilfeangelegenheiten ausüben darf.

Das Amt sagte zu, die technischen und organisatorischen Maßnahmen zur Abschottung der Beihilfestelle im Sinne des § 90a BBG zu verbessern und hat die organisatorische Eingliederung der Beihilfefeststellungsstelle inzwischen neu geregelt.

Diese Organisationsverfügung habe ich wie folgt bewertet:

Zu begrüßen ist, daß

– die Fachaufsicht über die Beihilfefeststellungsstelle nunmehr dem Leiter des Rechtsreferates übertragen ist,
– der mit der Dienstaufsicht betrauten Referatsleitung, deren Vorgesetzten und Vertretern jeglicher Zugang zu Unterlagen, die Beihilfeangelegenheiten betreffen, untersagt wird und
– die Rechtsberatung der Beihilfestelle durch das Justitiariat erfolgt.

Diese Neuregelung entspricht allerdings noch nicht der vom Gesetzgeber gewollten organisatorischen Trennung von der übrigen Personalverwaltung, da die Beihilfebearbeitung faktisch nach wie vor in einer Organisationseinheit der Personalverwaltung stattfindet. Mit der getroffenen Regelung wird lediglich formal sichergestellt, daß der Referatsleitung, die die Maßnahmen der Personalverwaltung und Personalwirtschaft vorbereitet und durchführt, sowie deren Vertretung eine Einsichtnahme in Beihilfeunterlagen untersagt wird.

Eine derartige Regelung ist zwar für einen gewissen Übergangszeitraum hinnehmbar, für eine große Behörde wie das Deutsche Patentamt als Dauerlösung jedoch nicht akzeptabel. Der Gesetzgeber hat die mit der Organisationsverfügung vorgegebene Lösung nur für kleinere personalverwaltende Behörden vorgesehen, in denen ein Sachbearbeiter mit der Bearbeitung von Beihilfevorgängen nicht ausgelastet ist (vgl. BT-Drs. 12/544 S. 17). Meines Erachtens wäre vor allem mit Blick auf die Größe und die Mitarbeiterzahl des Deutschen Patentamtes auch eine organisatorische Angliederung der Beihilfestelle an eine andere Organisationseinheit möglich, ohne zusätzliche Mitarbeiter dafür einzustellen, zumal beim Deutschen Patentamt zwei Mitarbeiter ausschließlich mit der Bearbeitung von Beihilfeanträgen befaßt sind.

Ich habe das Deutsche Patentamt darauf hingewiesen, daß aus den genannten Gründen die konsequente Einhaltung der Vorgaben der Organisationsverfügung besonders wichtig ist. Darüber hinaus habe ich dringend empfohlen, mittelfristig die Beihilfestelle einer Organisationseinheit zuzuordnen, die mit der Vorbereitung und Umsetzung von Entscheidungen der Personalverwaltung und Personalwirtschaft nicht betraut ist,. Diese Organisationsmaßnahme würde sich auch vertrauensbildend auf das Verhältnis Personal – Personalverwaltung auswirken und zu einer größeren Akzeptanz bei den Mitarbeitern beitragen.

18.5.3 Abschottung von Daten bei der Vorprüfung in Besoldungs- und Beihilfeangelegenheiten

Die Frage der Abschottung von Beihilfedaten stellt sich nicht nur bei der Beihilfestelle selbst, sondern auch für die Vorprüfungsstellen. So hatte ich zu bewerten, ob es zulässig ist, daß derselbe Bearbeiter der Vorprüfungsstelle sowohl im Bereich der Personalverwaltung als auch der Beihilfestelle prüft.

Die Abschottung der Beihilfedaten auch im Zusammenhang mit der Vorprüfung ist nicht zwingend. Zweck der Abschottung ist es, die bei der Beihilfebearbeitung regelmäßig anfallenden personenbezogenen Daten gegen unbefugte Kenntnisnahme abzusichern (vgl. BT-Drs. 12/544 S. 17). Die Kenntnisnahme von Daten über Krank-

heiten, Diagnosen, Behandlungen und Medikationen ist daher im Rahmen des Beihilfeverfahrens auf das für die Abrechnung unumgänglich notwendige Maß zu beschränken. Insbesondere gegenüber Personen, die Personalentscheidungen treffen oder daran mitwirken, sind Beihilfedaten abzuschotten.

Die Vorprüfungsstellen kontrollieren die Rechtmäßigkeit des Verwaltungshandelns (vgl. Nr. 1.4 VPOB); sie treffen keine Sachentscheidungen, etwa in Beihilfe- oder Personalangelegenheiten. Daneben sollen sie beurteilen, ob das Verwaltungshandeln, soweit es sich finanziell ausgewirkt hat oder auswirken kann, bei gleichgelagerten und zusammengehörenden Sachverhalten organisatorisch sinnvoll ist. Die Gefahr der Zweckentfremdung der kontrollierten personenbezogenen Daten besteht hier nicht.

Allerdings ist zu beachten, daß das gesetzliche Abschottungsgebot des § 90a BBG durch Art und Inhalt der Vorprüfungsniederschrift nicht unterlaufen wird. Eine Prüfungsmitteilung oder Beanstandung, die einen Aufgabenbereich außerhalb der Beihilfebearbeitung betrifft oder an ihn gelangt, darf nicht personenbezogene Erkenntnisse enthalten oder verwerten, die bei einer Prüfung der Beihilfestelle gewonnen wurden. Insoweit strahlt das Abschottungsgebot auch auf die Vorprüfungsstelle aus. § 90a BBG steht der Vorprüfung von Personalverwaltung und Beihilfe durch eine Person nicht entgegen, wenn meiner Empfehlung gefolgt wird.

Seit 1. Januar 1998 gibt es keine Vorprüfungsstellen mehr, sondern Prüfungsämter. Diese sind der Dienst- und Fachaufsicht des Bundesrechnungshofes unterstellt. Für sie gelten die gleichen Grundsätze.

18.5.4 Zustellung von Beihilfe-Widerspruchsbescheiden

Eine Bundesbehörde hatte sich mit datenschutzrechtlichen Bedenken gegen die Zustellung von Widerspruchsbescheiden im Beihilferecht nach § 5 Verwaltungszustellungsgesetz (VwZG) an mich gewandt.

Danach werden die Bescheide so zugestellt, daß ein Bediensteter dem Empfänger das Schriftstück aushändigt und dieser ein mit dem Datum versehenes Empfangsbekenntnis unterschreibt. Außerdem vermerkt der zustellende Bedienstete das Datum der Zustellung auf dem Schriftstück. Die Behörde läßt Widerspruchsbescheide durch den jeweiligen Vorgesetzten aushändigen, so daß dieser – sofern dies offen geschieht – die Möglichkeit hat, den Inhalt des Schriftstücks und somit der besonders schützenswerten Beihilfedaten zur Kenntnis zu nehmen.

Ich teile die Bedenken gegen diese Art der Zustellung eines Widerspruchsbescheides, da das Verfahren mit dem Abschottungsgebot des § 90a BBG nicht vereinbar ist.

Ich habe das für das Beihilfeverfahren generell zuständige BMI darauf hingewiesen, daß meine Bedenken im Rahmen der Ermessensentscheidung nach § 2 Abs. 2 VwZG über die zu wählende Zustellungsart zu berücksichtigen sind und habe empfohlen, § 5 VwZG bei der Zustellung von Widerspruchsbescheiden im Beihilferecht in den hier gegebenen Fällen (Zustellung durch den Vorgesetzten) nicht mehr anzuwenden.

Das BMI hat mir bestätigt, daß das Verwaltungszustellungsgesetz eine Aussage darüber, welche Bedienstete für Zustellungen herangezogen werden können, nicht trifft. Die Zustellung nach § 5 VwZG sei nur eine von mehreren dort vorgesehenen Zustellungsarten. Daher könne, um datenschutzrechtlichen Forderungen gerecht zu werden, in den genannten Fällen nach pflichtgemäßem Ermessen eine andere Form der Zustellung gewählt werden.

Die anfragende Bundesbehörde hat das Verfahren der Zustellung von Widerspruchsbescheiden im Beihilferecht jetzt so geregelt, daß der Widerspruchsbescheid gegen Empfangsbekenntnis auszuhändigen und das Aushändigungsdatum auf dem verschlossenen Umschlag zu vemerken ist.

Eine sowohl § 5 VwZG als auch den Belangen des Datenschutzes genügende Zustellungspraxis wäre schließlich auch dann anzunehmen, wenn der Beihilfesachbearbeiter oder der Bearbeiter des Widerspruchsverfahrens die Zustellung selbst bewirken.

18.5.5 Beihilfeverfahren im Auslandsschuldienst

Aufgrund verschiedener Eingaben habe ich mich mit dem Beihilfeverfahren für Lehrer im Auslandsschuldienst auseinandergesetzt. So haben Petenten problematisiert, daß für die Abrechnung von Beihilfen der beamteten Lehrer Rezepte und Arztrechnungen dem Verwaltungsleiter der Schule offen vorzulegen sind, damit dieser auf den Belegen die Umrechnung aus der jeweiligen Landeswährung in DM bestätigt. Dann wird der Beihilfeantrag mit den Belegen zur erneuten Kontrolle der Umrechnung an die Deutsche Botschaft des Landes in einem offenen Umschlag weitergeleitet und danach erst an die zuständige Beihilfestelle im Bundesverwaltungsamt gesandt.

Auch hier kommt der Abschottung der Beihilfestelle und des Verfahrens, mit dem Ansprüche auf Beihilfe geltend gemacht werden, gegenüber der Personalverwaltung (s. o. Nr. 18.5) entscheidende Bedeutung zu. Eine Kenntnisnahme von Beihilfedaten durch den Verwaltungsleiter der Schule des antragstellenden Lehrers ist mit § 90a BBG nicht zu vereinbaren.

Das BVA hat mir zu meinen Bedenken mitgeteilt, daß das Verfahren auf dem „Leitfaden für die Durchführung der Beihilfevorschriften (BhV) und der Vorschriften über die Gewährung von Beihilfen in Krankheits-, Geburts- und Todesfällen an Bundesbedienstete im Ausland (BhV-Ausland)“ des AA beruhe. Danach muß auf jedem einzelnen Beleg unter Angabe des Kurses der Rechnungsbetrag umgerechnet und von einem zur rechnerischen Feststellung befähigten Beamten oder Angestellten geprüft und festgestellt werden. Darüber hinaus würde eine verantwortliche Bestätigung zur Frage der Angemessenheit (Ortsüblichkeit) der von Ärzten des Gastlandes berechneten Honorare und der sonstigen im Einzelfall notwendigen Angaben erwartet, was ohne

Einsicht in die Beihilfeunterlagen nicht möglich sei. Der Leitfaden hebe hervor, daß die bei der Prüfung und Weiterleitung der Anträge bekanntgewordenen Daten geheimzuhalten sind.

Als Lösung für die Auslandsschule hat das BVA vorgeschlagen, sowohl die Umrechnung von Fremdwährungsbeträgen in DM als auch die Feststellung der ortsüblichen Angemessenheit der Aufwendungen für ärztliche und zahnärztliche Leistungen nur noch von dem zur rechnerischen Feststellung befähigten Beamten oder Angestellten der zuständigen Auslandsvertretung vornehmen zu lassen. Dieses Verfahren entspreche im übrigen dem Regelfall. Dadurch würde vermieden, daß Mitarbeiter – und damit auch der Verwaltungsleiter – der Auslandsschule die Beihilfedaten der Lehrer weiterhin zur Kenntnis bekommen.

Das BVA hat die Auslandsschulen auf das Datenschutzproblem und das zur Lösung mögliche Verfahren hingewiesen und um Information der betroffenen Lehrkräfte gebeten.

18.6 Umfang der Einsichtsrechte in Unterlagen von Assessment-Center-Verfahren

Eine Krankenkasse hatte nach einer Organisationsreform mehrere neu geschaffene Führungspositionen erstmals zu besetzen und sich entschlossen, im Rahmen der Bewerberauswahl ein Assessment-Center-Verfahren durchzuführen (siehe auch 14. TB Nr. 9.10, 15. TB Nr. 9.17).

In einem Mitarbeiterbrief wurden alle Mitarbeiter informiert, die Teilnahme am Assessment-Center sei Voraussetzung für eine Berücksichtigung bei der Besetzung der Führungsfunktionen, die Ergebnisse würden nur für die Entscheidung herangezogen, es gebe für die Teilnehmer abschließende Feedback-Gespräche und die Ergebnisse würden nicht in die Personalakte aufgenommen. Nach Abschluß des Verfahrens wurde jeder Bewerber in einem ausführlichen Einzelgespräch unter wörtlicher Verlesung des Gutachtens über sein Ergebnis unterrichtet. Wünschen auf Einsicht oder Aushändigung einer Kopie des Ergebnisses wurde nicht entsprochen.

Da der Sachverhalt in allen für die datenschutzrechtliche Bewertung wesentlichen Aspekten dem Assessment-Center-Verfahren entsprach, das die DTAG bei der Ausgliederung des Mobilfunkbereichs einsetzte (s. 15. TB Nr. 9.17), ergaben sich für meine Bewertung keine neuen Aspekte. Unterlagen aus dem Assessment-Center-Verfahren haben einen konkreten Bezug zu dem Dienst- bzw. Arbeitsverhältnis. Den Teilnehmern steht daher ein Einsichtsrecht nach § 90c BBG zu. Das Einsichtsrecht ist nicht einseitig durch den Arbeitgeber disponibel.

Die Teilnahme im Assessment-Center in Kenntnis des vorgesehenen Ablaufs bedeutet keinen wirksamen konkludent erklärten, unwiderruflichen Verzicht auf Einsichtsrechte. Einer solchen Annahme stünde auch § 6 Abs. 1 BDSG entgegen. Über die dort genannten unabdingbaren Rechte hinaus gilt die Unabdingbarkeit auch für bereichsspezifische Kodifizierungen des Einsichtsrechts.

Einen Ausschluß des Einsichtsrechts halte ich auch unter dem Gesichtspunkt, die Teilnehmer hätten in das ihnen vorher bekannte Verfahren insgesamt durch ihre Teilnahme konkludent eingewilligt, nicht für gerechtfertigt. Von einer wirksamen Einwilligung kann nicht ausgegangen werden, denn für die Betroffenen bestand tatsächlich ein faktischer Zwang zur Teilnahme, da sie andernfalls nicht zum Assessment-Center-Verfahren zugelassen worden wären und damit von der Bewerbung um die zu besetzenden Führungspositionen ausgeschlossen gewesen wären.

Das Einsichtsrecht schließt das Recht zur Fertigung von Abschriften oder Kopien (§ 90c Abs. 3 Satz 2 erster Halbsatz BBG) ein.

Was die weiteren während des Assessment-Center-Verfahrens im Vorfeld des Gutachtens entstandenen Unterlagen anbelangt, so ist eine Einsichtnahme der Betroffenen dann unzulässig, wenn ihre Daten mit den Daten Dritter derart verbunden sind, daß ihre Trennung nicht oder nur mit unverhältnismäßig großem Aufwand möglich ist, was beispielsweise gegeben ist, wenn auf einem Blatt handschriftliche Aussagen über mehrere Teilnehmer vermerkt sind. In diesem Fall hat der Teilnehmer zwar keinen Anspruch auf Einsicht in die Unterlagen, die ihn betreffenden Daten müssen ihm dann jedoch auf anderem Wege mitgeteilt werden.

Die Krankenkasse teilt meine Beurteilung nicht. Sie hat mir mitgeteilt, daß sie an ihrer Auffassung festhält. Sie will jedoch bei weiteren Assessment-Center-Verfahren die aus ihm resultierenden Ergebnisse zu den Personalakten nehmen, um sie auch später zu berücksichtigen. Damit erhielte der Betroffene auch Einsicht. Zur Frage, ob Gutachten aus dem Assessment-Center-Verfahren zu den Personalakten genommen werden dürfen, habe ich mich bereits früher eingehend geäußert (s. 15. TB Nr. 9.17). Meines Erachtens muß dies der alleinigen und freiwilligen Entscheidung des Betroffenen überlassen bleiben.

18.7 Darf der Untersuchungsführer im Disziplinarverfahren von mir kontrolliert werden?

Gegen eine Petentin lief ein disziplinarrechtliches Vorermittlungsverfahren. Mit ihrer Eingabe wandte sie sich gegen Datenerhebungen durch den Untersuchungsführer. Eine Zeugenbefragung im Wohnort der Petentin hatte nämlich dazu geführt, daß das Vorermittlungsverfahren in ihrem privaten Umfeld bekannt wurde.

Eine Besonderheit des Disziplinarverfahrens ist, daß die Bundesdisziplinarordnung dem Disziplinargericht die – regelmäßig genutzte – Möglichkeit einräumt, auf eine eigene Beweisaufnahme zu verzichten, damit die in der Untersuchung nach §§ 56ff. BDO durchgeführte Beweiserhebung nicht in der Hauptverhandlung des Gerichts wiederholt werden muß. Diese Beweiserhebung ist Teil der gerichtlichen Beweisaufnahme und insoweit eine Vorwegnahme der Hauptverhandlung. Deshalb stellt die BDO sicher, daß die Beweismittel in einem quasi-richterlichen Verfahren erhoben werden. Der

Untersuchungsführer erhebt die Beweise somit in richterlicher Funktion. Der mit richterlicher Unabhängigkeit ausgestattete Untersuchungsführer hat zur Aufklärung der materiellen Wahrheit alleinverantwortlich zu entscheiden, in welcher Form und auf welche Art und Weise er Beweise erheben will. Wenn es zur Sicherung des Beweises erforderlich ist, darf der Untersuchungsführer Zeugen und Sachverständige sogar eidlich vernehmen.

Nach § 21 BDSG darf sich jedermann an mich wenden, *„wenn er der Ansicht ist, bei der Erhebung, Verarbeitung oder Nutzung seiner personenbezogenen Daten durch öffentliche Stellen des Bundes in seinen Rechten verletzt worden zu sein. Für die Erhebung, Verarbeitung oder Nutzung von personenbezogenen Daten durch Gerichte des Bundes gilt dies nur, soweit diese in Verwaltungsangelegenheiten tätig werden.“*

Damit unterfällt die Rechtsprechung der Gerichte nicht meiner Kontrolle.

Daher gilt m.E. § 21 Satz 2 BDSG, der der Wahrung der richterlichen Unabhängigkeit dient, auch für die Vorermittlungen des Untersuchungsführers nach §§ 56ff. BDO. Im konkreten Fall war mir damit eine Kontrolle entzogen.

18.8 Sozialgeheimnis bei der Beurteilung von Geschäftsführern gebrochen?

Mir wurde vorgetragen, daß die Geschäftsführer einer Ersatzkasse nach vorgegebenen Beurteilungskriterien zunächst von einem Revisor beurteilt werden.

Nach den internen Anweisungen der Kasse sind den Revisoren von den Kassen sämtliche für die Prüfung erforderlichen Unterlagen (z. B. Buchhaltungsunterlagen, Kassenbelege, Geschäftsvorgänge der Kasse – einschließlich der Leistungsakten – und des Verbandes der Angestellten-Krankenkassen) vorzulegen, was für die Aufgabenerfüllung der Innenrevision erforderlich ist. Zusätzlich ist den Revisoren die Erstbeurteilung der Geschäftsführer sowie die Zweitbeurteilung von deren Stellvertretern übertragen. § 35 Abs. 1 Satz 3 SGB I sieht aber vor, daß Sozialdaten der Beschäftigten und ihrer Angehörigen Personen, die Personalentscheidungen treffen oder daran mitwirken können, weder zugänglich sein noch von Zugriffsberechtigten weitergegeben werden dürfen.

Mit der Beteiligung am Beurteilungsverfahren wirkt der Revisor an Personalentscheidungen bzw. an deren Vorbereitung mit.

Das dargestellte Beurteilungssystem kann dazu führen, daß in die konkreten Beurteilungbeiträge der Revisoren sachfremde Erwägungen einfließen, die auf der Kenntnis von Leistungsunterlagen, beispielsweise Arbeitsunfähigkeitszeiten, Erkrankungen der Betroffenen oder deren Familienangehörigen, beruhen.

Ich habe der Kasse empfohlen, eine den Anforderungen des § 35 Abs. 1 Satz 3 SGB I gerecht werdende Lösung zu suchen, wonach künftig der Revisor, der die Beurteilung eines Geschäftsführers bzw. dessen Vertreters wahrnimmt, keinen Zugriff auf die Leistungsunterlagen dieser Führungskräfte nehmen wird. Mit der Prüfaufgabe sollte künftig ein anderer Revisor betraut oder bei Bedarf die Prüfung dieser Leistungsunterlagen in anderer Weise sichergestellt werden. Die Kasse hat zugesagt, ihr Verfahren meinen Empfehlungen entsprechend neu zu gestalten.

18.9 Automatisierte Personaldatenverarbeitung

Auch in der Bundesverwaltung setzt sich mit dem zunehmenden Einsatz von Informationstechnik der Trend fort, personenbezogene Daten von Mitarbeitern automatisiert zu verarbeiten. Dabei bleiben auch datenschutzrechtliche Probleme nicht aus.

18.9.1 Personaldatenverarbeitung des BAFl beanstandet

Im Berichtszeitraum habe ich die Zentrale des BAFl im Hinblick auf die automatisierte Personaldatenverarbeitung beraten und kontrolliert (s. auch 15. TB Nr. 9.7.5). Bei meiner früheren Kontrolle habe ich trotz festgestellter Mängel auf eine förmliche Beanstandung nach § 25 BDSG verzichtet und dem BAFl mehrere Empfehlungen zur Verbesserung der Personaldatenverarbeitung gegeben. Deren Umsetzung habe ich jetzt kontrolliert und u. a. folgendes festgestellt:

- Die inzwischen in Kraft gesetzte Dienstanweisung enthielt zahlreiche Abweichungen von der mit mir und dem Gesamtpersonalrat im Anschluß an die Kontrolle von 1994 abgestimmten Dienstanweisung zur (automatisierten) Personaldatenverarbeitung.

  So mußte ich feststellen, daß das BAFl den Entwurf der Dienstanweisung mit dem Hinweis, er sei mit mir abgestimmt, dem Gesamtpersonalrat zugeleitet hatte, der ihm daraufhin zustimmte. Selbst der mit dem Personalrat abgestimmte Entwurf wurde bereits zum Zeitpunkt der Übersendung an mich, aber auch danach, noch erheblich geändert. Weder der Gesamtpersonalrat noch ich wurden hierüber informiert.

  Über die inhaltlichen Defizite hinaus habe ich dieses Vorgehen als nicht vereinbar mit § 24 Abs. 4 BDSG bewertet, nach dem die öffentlichen Stellen des Bundes verpflichtet sind, mich bei der Erfüllung meiner Aufgaben zu unterstützen, und habe erneut gefordert, die Dienstanweisung unter Berücksichtigung des damals mit mir abgestimmten Entwurfs zu überarbeiten. Dem hat das BAFl inzwischen entsprochen.

- Zahlreiche Dateien und Auswertungen waren erstellt worden, die unstreitig für eine Verhaltens- oder Leistungskontrolle der Mitarbeiter geeignet sind und damit nach § 75 Abs. 3 Nr. 17 Bundespersonalvertretungsgesetz der Mitbestimmung der Personalvertretung unterliegen, die jedoch nicht beteiligt war.

- Stichprobenartig habe ich an PC in den Personalreferaten Personaldateien, Auswertungen sowie die erforderlichen technischen und organisatorischen Maßnahmen nach § 9 BDSG sowie der Anlage hierzu kontrolliert. Hierbei habe ich zahlreiche Mängel festgestellt.

Für meine Bewertung war von Bedeutung, daß es sich vielfach um Datenschutzverstöße im Umgang mit besonders schützenswerten Daten – Personaldaten bzw. Personalaktendaten – handelt, deren Abstellung von mir bereits im Jahr 1994 gefordert und vom BAFl damals zugesagt worden war. Ich habe deshalb die zahlreichen festgestellten Mängel bei den technischen und organisatorischen Maßnahmen, insbesondere den fehlenden Zugriffsschutz bei den dem Personalaktengeheimnis unterliegenden Mitarbeiterdaten, nach § 25 Abs. 1 BDSG als Verstoß gegen § 9 und der Anlage zu § 9 Satz 1 BDSG gegenüber dem BMI **beanstandet**.

Nach den mir vom BMI inzwischen übersandten Berichten sowie umfangreichen Unterlagen habe ich festgestellt, daß das BAFl die von mir beanstandeten Mängel behoben bzw. deren Behebung eingeleitet hat, um die gesetzlichen Vorgaben sicherzustellen.

18.9.2 Verarbeitung von Beurteilungsnoten

In datenschutzrechtlichen Eingaben von Beschäftigten und im Zusammenhang mit meiner Beratung von Bundesbehörden bei der Einführung oder Umstellung von Systemen der automatisierten Personaldatenverarbeitung wurde mir wiederholt die Frage gestellt, ob die Verarbeitung von Beurteilungsnoten rechtmäßig sei.

Ich habe darauf hingewiesen, daß das Bundesverwaltungsgericht bereits am 3. September 1987 (RDV 1988, 203) zur Zulässigkeit der Speicherung von Platzziffern in automatisierten Personaldatensystemen entschieden hat, daß dies im Rahmen des Verfahrens PERFIS (Personalführungs- und -informationssystem für Soldaten) des Bundesministeriums der Verteidigung zulässig ist.

Diese Entscheidung hatte mich dazu veranlaßt, meine in früheren Tätigkeitsberichten (zuletzt 9. TB Nr. 7.2.1) vertretene Auffassung zu überdenken, nach der von der automatisierten Verarbeitung der Beurteilungsnoten abzusehen ist, sofern diese sich nicht nur auf eine Speicherung zur Einzelanzeige am Bildschirm beschränkt.

Ich halte die automatisierte Verarbeitung von Beurteilungsnoten (beispielsweise in einem Personalinformationssystem) dann für zulässig, wenn sichergestellt ist, daß sie für Zwecke der Personalverwaltung oder Personalwirtschaft erforderlich und nicht alleinige Grundlage für Personalentscheidungen ist. Dies setzt voraus, daß bei Personalentscheidungen stets auch die Personalakte herangezogen wird.

Diese Rechtsauffassung wird auch durch § 90 Abs. 4 BBG reflektiert. Danach dürfen beamtenrechtliche Entscheidungen nicht ausschließlich auf Informationen und Erkenntnisse gestützt werden, die unmittelbar durch automatisierte Verarbeitung personenbezogener Daten gewonnen werden. In der Begründung zu dieser Norm heißt es, daß der Datenverarbeitung (auch von Beurteilungsnoten) im Rahmen automatisierter Personalverwaltungssysteme nur eine dienende Rolle zukommt. Sie muß sich danach auf Hilfs- und Unterstützungsfunktionen beschränken. Das Ergebnis einer solchen Verarbeitung – so die Begründung – darf deshalb nicht ausschließlich Grundlage einer Personalentscheidung sein. Ein Verbot, Beurteilungsdaten automatisiert zu verarbeiten, läßt sich hieraus nicht ableiten. Ich habe daher bei Kontrollen und bei der Beratung zur Einführung neuer automatisierter Systeme die Verarbeitung von Beurteilungsdaten aus datenschutzrechtlicher Sicht dann akzeptiert, wenn die o.a. Voraussetzungen gegeben waren und die Zustimmung der Personalvertretung vorlag.

Zur Frage, ob eine angefochtene Beurteilung in einem solchen System als streitbefangen zu kennzeichnen ist, verweise ich auf meine im 14. TB (Nr. 9.7) dargestellte Rechtsauffassung. Danach ist sie bis zu einer endgültigen Entscheidung in der Personalakte als streitbefangen zu kennzeichnen und diese Tatsache bei Personalmaßnahmen gebührend zu berücksichtigen. Zur Personalakte gehören nach § 90 Abs. 1 BBG auch Personalaktendaten in Dateien, also auch in einem Personalinformationssystem.

18.9.3 Datenschutzrechtlich wünschenswerte Dienstvereinbarungen

Das Bundeskanzleramt hat mir eine zwischen einem Ministerium und seinem Personalrat abgeschlossene Dienstvereinbarung über den Einsatz von Informations- und Kommunikationstechniken übersandt und mich um Stellungnahme hierzu gebeten. Nachfolgend fasse ich die wichtigsten Punkte meiner Antwort an das BK zusammen.

Derartige Vereinbarungen sollten nicht nur die Einführung und Anwendung von Datenverarbeitungsverfahren für Personaldaten regeln. Sie sind vor allem geeignet, die Persönlichkeitsrechte der Bediensteten abzusichern. In diesen Dienstvereinbarungen können insbesondere die allgemeinen Vorschriften des BDSG und des BBG (§§ 90ff.) konkretisiert werden. Dies trägt ganz entschieden dazu bei, die Akzeptanz der automatisierten Personaldatenverarbeitung zu erhöhen und künftigen Auseinandersetzungen wirksam vorzubeugen. Die Dienstvereinbarungen (und Dienstanweisungen) sollten die jeweils vorhandenen Bedingungen, die tatsächlichen Systemumgebungen sowie die konkreten Ausgestaltungen der Systeme zur automatisierten Personaldatenverarbeitung berücksichtigen.

Zur Ausgestaltung von Dienstvereinbarungen zur automatisierten Personaldatenverarbeitung habe ich mehrfach in meinen Tätigkeitsberichten (insbesondere 10. TB Nr. 7.4.3) Stellung genommen. Ich habe frühzeitig darauf hingewiesen, daß in Fällen der Mitbestimmungsbedürftigkeit die fehlende Beteiligung des Personalrates zur Unzulässigkeit der Datenverarbeitung führen kann und auf ein Urteil des BAG aufmerksam gemacht, nach dem unter Verstoß gegen Mitbestimmungsrechte erhobene Daten nicht gespeichert werden dürfen (10. TB Nr. 4.2). Aufgrund der Rechtsprechung ist inzwischen unstreitig, daß die Einführung und Anwendung technischer Einrichtungen nach § 75 Abs. 3 Nr. 17 BPersVG dann der Mitbestimmung unterliegen, wenn diese für eine Verhaltens- und Leistungskontrolle der Mitarbeiter **geeignet** sind (vgl. z. B. BVerwG vom 16. Dezember 1987, RDV 1988 S. 201, und vom 23. September 1992, RDV 1993 S. 68).

18.10 Personalrechtliche Eingaben, die ich bei den verantwortlichen Stellen beanstandet habe

18.10.1 Abgabe von Schreiben sensiblen Inhalts

Vielfach liegt es im Interesse des Bürgers, wenn eine für sein Anliegen unzuständige Behörde sein Schreiben ohne weiteres an die zuständige Behörde abgibt. Daß das aber auch nicht unbedacht geschehen darf, zeigt das folgende Beispiel:

Ein Beamter des AA, der in einem deutschen Konsulat im Ausland eingesetzt war, trug sich mit dem Gedanken, vorzeitig aus dem Dienst auszuscheiden. Mit der Bitte um Auskunft über die Höhe seiner bereits erworbenen Pensionsansprüche wandte er sich deswegen an die OFD Düsseldorf, von der er wußte, daß sie eine zentrale Zuständigkeit für die Zahlung von Versorgungsbezügen an Empfänger im Ausland hatte. Für die Erstfestsetzung der Versorgung ist jedoch das AA zuständig. Also leitete die OFD Düsseldorf das Schreiben des Petenten dorthin weiter und so erfuhr die Personalstelle des Petenten, daß er erwog, vorzeitig auszuscheiden.

Der Petent erhielt von der OFD Düsseldorf eine Abgabenachricht, d. h. sie informierte ihn darüber, daß sie sein Schreiben an das AA weitergeleitet hatte. Die Abgabenachricht adressierte die OFD Düsseldorf jedoch nicht an den Petenten persönlich, sondern an das Konsulat, bei dem der Petent arbeitete, lediglich mit dem Zusatz „z.Hd. ...“. Derart adressierte Sendungen werden üblicherweise von der Poststelle geöffnet und dem Empfänger im Geschäftsgang zugeleitet – mit der Folge, daß der Inhalt in der Dienststelle bekannt wird.

Datenschutzrechtlich problematisch war jedoch nicht nur die Adressierung der Abgabenachricht, sondern auch die ungefragte Abgabe der Anfrage des Petenten an das AA. Die Abgabe eines Schreibens an die zuständige Behörde ist datenschutzrechtlich eine Übermittlung. Sie ist zulässig, wenn ihr nicht überwiegende schutzwürdige Interessen des Betroffenen entgegenstehen. In dem Schreiben hat der Absender Erwägungen über seine persönlichen beruflichen Zukunftspläne außerhalb seiner aktuellen Beschäftigung offengelegt, die besonders schützenswert sind. Es ist erkennbar nicht für das Personalreferat bestimmt. Das Schreiben hätte folglich nicht weitergegeben werden dürfen.

Das BMF antwortete erst einmal, die „irrtümliche“ Adressierung entspreche keineswegs der üblichen Verwaltungspraxis, sondern beruhe auf einem Kanzleiversehen. Dieses sei zum Anlaß genommen worden, die Kanzlei entsprechend zu sensibilisieren.

Allerdings gehört die Auswahl der richtigen Anschrift nicht zu den Aufgaben der Kanzleikräfte. Die Verantwortung für den sachlichen Inhalt der Entwürfe trägt stets der Zeichnende. Deshalb hat die OFD Düsseldorf auf Veranlassung des BMF schließlich die verantwortlichen Bediensteten auf diese Fehlerquelle hingewiesen.

Das BMF berief sich in einer weiteren Stellungnahme auf eine Vorschrift in der Geschäftsordnung für die OFDen, wonach Sendungen, für deren Erledigung die empfangene OFD nicht zuständig ist, an die zuständige Stelle weiterzuleiten sind; die Abgabe somit zulässig gewesen sei. Daher mußte ich befürchten, daß die OFD Düsseldorf und andere Stellen im Geschäftsbereich des BMF in vergleichbaren Fällen auch künftig Schreiben – ungeachtet der Sensibilität ihres Inhalts – an die zuständigen Stellen abgeben werden. Deshalb habe ich beim BMF die Behandlung der Anfrage des Petenten durch die OFD Düsseldorf förmlich **beanstandet**, weil die OFD gegen §§ 4 Abs. 1, 12 Abs. 4 und 28 BDSG verstoßen hat. Das BMF hat mir aufgrund der Beanstandung mitgeteilt,daß es beabsichtigt, die Geschäftsordnung für die Oberfinanzdirektionen entsprechend zu ergänzen.

18.10.2 Verhärtete Fronten

Die Kosten des Personalrats trägt die Dienststelle. Das gilt auch für die Kosten der Dienstreisen seiner Mitglieder, soweit sie zur Erfüllung ihrer Aufgaben notwendig sind (§ 44 BPersVG). Die Feststellung, was „notwendig“ ist, birgt naturgemäß Konfliktpotential zwischen Dienststelle und Personalrat. Denn einerseits ist von der Rechtsprechung anerkannt, daß der Dienststelle aus ihrer Verantwortung für den Bundeshaushalt die Befugnis und Pflicht erwächst, die sachliche Berechtigung der Reisekostenabrechnungen zu überprüfen. Andererseits darf dies nicht zu einer Ausforschung der Personalratstätigkeit führen.

Diese schwierige Gratwanderung war Anlaß für eine Eingabe aus dem Bereich des BMV. Der Petent war Mitglied des Hauptpersonalrats und Beamter des Bundesamtes für Seeschiffahrt und Hydrographie (BSH). Um die Berechtigung von zehn seiner Reisekostenabrechnungen zu überprüfen, hatte das BSH den Vorsitzenden des Hauptpersonalrats gebeten zu bestätigen, daß die zehn in dem Schreiben aufgeführten Dienstreisen zur Erfüllung der Aufgaben als Mitglied des Personalrats i.S.v. § 44 Abs. 1 BPersVG notwendig waren. Das Schreiben enthielt Angaben über den Erkenntnisstand nach Aktenlage des BSH und bewertende Hinweise („außergewöhnlich häufig"), aus denen Zweifel des BSH an der Berechtigung der Reisekostenrechnungen des Petenten für den Vorsitzenden des Hauptpersonalrats erkennbar waren. Zudem waren Kopien der Reisekostenrechnungen beigefügt, aus denen Einzelheiten erkennbar waren, die im Hinblick auf die Fragestellung ohne Bedeutung sind.

Da der Dienstherr ein Prüfungsrecht hinsichtlich der Notwendigkeit von Dienstreisen der Personalratsmitglieder hat, habe ich an sich keine Bedenken gegen eine Nachfrage über Ort und Zeit von Sitzungsterminen beim Vorsitzenden des Personalrats, wenn insoweit konkrete Zweifel an der Richtigkeit der Angaben des Betroffenen bestehen. Zulässig ist aber nur die Erhebung erforderlicher personenbezogener Daten, nicht aber die Offenbarung von über den für die Fragestellung notwendigen Umfang hinausgehenden personenbezogenen Daten. Auch verbleibt die rechtliche Bewertung der „Notwendigkeit“ von Kosten und Sachaufwand nach § 44 BPersVG in der Zuständigkeit des Dienstherrn. Die Fragestellung im Schreiben des BSH hätte gezielt darauf be-

schränkt werden können, ob, an welchem Ort und in welchem zeitlichen Umfang der Petent an den von den Reisekostenrechnungen betroffenen Tagen Personalratstätigkeit ausgeübt hat. Das Schreiben des BSH ging darüber hinaus. Anstelle konkreter sachverhaltlicher Fragen enthielt es die Bitte an den Vorsitzenden des Hauptpersonalrats zu bestätigen, daß die Reisen des Petenten notwendig waren. Zudem waren aus den anliegenden Kopien der Reisekostenrechnungen personenbezogene Daten zu ersehen, die nicht hätten offenbart werden dürfen. Schon aus diesen Gründen habe ich die Erhebung beim Vorsitzenden des Hauptpersonalrats daher im Ergebnis als unzulässig bewertet. Das Verwaltungsgericht Hamburg hat in einem den Rückforderungsbescheid des BSH rechtskräftig aufhebenden Beschluß zudem die Zuständigkeit des BSH für Reisekostenrechnungen des Petenten in seiner Eigenschaft als Mitglied des Hauptpersonalrats verneint.

Zudem sollte der Betroffene von der Dienststelle über die ohne seine Mitwirkung erfolgte Erhebung informiert werden, sobald dies ohne Beeinträchtigung des Erhebungszweckes möglich ist. Es entspricht dem Willen des Gesetzgebers, daß im Falle der Erteilung von Auskünften an Dritte nach § 90d BBG Empfänger und Inhalt der Auskunft dem Beamten schriftlich mitzuteilen sind (vgl. Begründung des Regierungsentwurfs zu § 90d BBG, BT-Drs. 12/544 Seite 20).

Begünstigt durch die Fragestellung und den aus dem Schreiben des BSH erkennbaren Zweifeln an der Berechtigung der Reisekostenrechnungen sah sich der Vorsitzende des Hauptpersonalrats zu Überprüfungen veranlaßt, die eigentlich ausschließlich der Reisekostenstelle des BSH oblagen. In einer Besprechung der Beamtengruppe des Hauptpersonalrats warnte der Vorsitzende unter Hinweis darauf, er hätte einen Prüfauftrag zu den Reisekostenabrechnungen des Petenten erhalten, davor, ihn zum Gruppensprecher zu wählen. Hierin lag eine unzulässige zweckändernde Nutzung der dem Vorsitzenden des Hauptpersonalrats vom BSH übermittelten Daten.

Der Hauptpersonalrat sah aufgrund des schwebenden Verdachts gegen den Petenten davon ab, ihn zur Freistellung vorzuschlagen. In einem personalvertretungsrechtlichen Beschlußverfahren erreichte der Petent die Feststellung des OVG Münster gegen den Hauptpersonalrat, daß die Zurückstellung des Freistellungsantrages durch den Personalrat allenfalls gerechtfertigt sein könne, wenn es sich um die Feststellung schwerwiegender Dienstvergehen handele, die im förmlichen Disziplinarverfahren verfolgt werden. Daraufhin teilte das BMV dem Hauptpersonalrat schriftlich mit, daß gegen den Petenten inzwischen eine Disziplinarverfügung in Form einer Geldbuße verhängt worden sei. Der Petent wurde darüber nicht informiert. In seiner Stellungnahme an mich verwies das BMV darauf, diese Auskunft sei auch im Interesse des Betroffenen erforderlich gewesen, um dem Hauptpersonalrat mitzuteilen, daß ein Hindernis im Sinne der Entscheidung des OVG nicht vorliege. Dafür hätte es genügt zu bestätigen, daß ein schwerwiegendes Dienstvergehen nicht vorliegt, das im förmlichen Disziplinarverfahren verfolgt wird. Damit wäre offen geblieben, ob ein Dienstvergehen überhaupt vorliegt. Die Tatsache der Verhängung einer Disziplinarverfügung, deren Art und Höhe sind geschützte Personaldaten. Die Mitteilung des BMV an den Hauptpersonalrat war unzulässig.

Zur Berechtigung der Disziplinarverfügung schwebte zwischen dem Petenten und dem BMV ein Rechtsstreit. Wegen einzelner Vorwürfe zu seinen Reisekostenrechnungen hatte der Petent sich in seinen Schriftsätzen auf die bisher unbeanstandete gleiche oder sogar weitgehendere Praxis anderer Personalratsmitglieder bezogen. Das BMV fertigte eine auszugsweise Kopie dieser Passagen des Schriftsatzes und sandte sie an den Hauptpersonalrat zur Stellungnahme. Dabei gab das BMV an, daß es sich um den Auszug aus einem Schreiben „in einer Personalangelegenheit von Herrn <Nachname des Petenten>“ handele.

Der Schriftverkehr zu einer Disziplinarsache unterliegt dem Personaldatenschutz. Er darf Personen, die mit der Bearbeitung der Angelegenheit nicht befaßt sind, nicht zugänglich gemacht werden. Schon die Tatsache, daß gegen einen Bediensteten ein Disziplinarverfahren anhängig ist, unterliegt dem Personaldatenschutz. Das gilt grundsätzlich auch schon dann, wenn die Behörde zu prüfen beginnt, ob eine Disziplinarmaßnahme berechtigt sein könnte. Denn auch in der bloßen Bestätigung vermuteter Sachverhalte kann eine unbefugte Offenbarung von personenbezogenen Daten liegen.

Die festgestellten datenschutzrechtlichen Verstöße habe ich gegenüber dem BMV und dem Hauptpersonalrat förmlich **beanstandet**.

Gegenüber dem Hauptpersonalrat habe ich die Beanstandung ausgesprochen, da ein Personalratsmitglied in einem öffentlich-rechtlichen Amtsverhältnis steht, aus dem sich bei Wahrnehmung von Personalratstätigkeit keine besonderen Pflichten gegenüber dem Dienstherrn ableiten lassen. Für Datenschutzverstöße in Wahrnehmung von Personalratstätigkeit ist das Personalratsmitglied nicht der Dienststelle gegenüber verantwortlich, sondern nur unmittelbar dem Betroffenen gegenüber.

19 Sozialwesen – Allgemeines

19.1 § 67e SGB X: Erster Schritt zu einer zentralen Datenabgleichsvorschrift?

Um der Mißbrauchsbekämpfung in allen Sozialleistungsbereichen ein schlagkräftiges Instrument an die Hand zu geben, hatte das BMA das Ziel verfolgt, eine zentrale Datenabgleichsvorschrift in das Datenschutzkapitel des SGB X aufzunehmen. Der mir vorgelegte Entwurf wäre allerdings weit über das Ziel hinausgeschossen und hätte das System der sozialdatenschutzrechtlichen Übermittlungsvorschriften in Zweiten Kapitel SGB X und viele bereichsspezifischen Datenschutzvorschriften in den anderen Büchern praktisch obsolet gemacht. Angesichts seiner generalklauselartigen Weite und mangelnden Differenzierung konnte ich diesen Entwurf daher nicht mittragen. Die Vorschrift sah weder

Protokollierungen der Abgleiche noch andere Ansätze für eine besondere Datenschutzkontrolle vor und berücksichtigte auch nicht, daß Datenabgleiche für Bürger transparent bleiben sollten. Leider zeigte sich das BMA nur zu sehr geringen Änderungen an seinem Entwurf bereit, den es dann noch als „sehr eilbedürftig“ einstufte und ihn mit Nachdruck weiterverfolgte.

Da ich mich nicht auf eine bloße Ablehnung des Entwurfs des BMA beschränken wollte, habe ich einen eigenen Entwurf der aus meiner Sicht erforderlichen Regelungsgegenstände für eine zentrale Datenabgleichsvorschrift zur Diskussion gestellt. Dabei ging es mir darum, durch Vorgaben zur Automatisierung, Zentralisierung und Flüchtigkeit des Abgleichsverfahrens die persönliche Kenntnisnahme von Sozialdatenprofilen durch Bearbeiter möglichst zu vermeiden und die datenschutzrechtliche Kontrollierbarkeit der Abgleiche zu gewährleisten. Da es beispielsweise ein Unterschied ist, ob ein BAföG-Amt und eine Wohngeldstelle einen Datenabgleich auf örtlicher Ebene einrichten wollen oder ob ein Datenabgleich unter Beteiligung der Datenstelle der Rentenversicherungsträger und der Bundesanstalt für Arbeit installiert werden soll, hielte ich differenzierte Rahmenvorgaben für Umfang und Verfahren solcher Datenabgleiche für erforderlich. Weiter ist für mich unverzichtbar, daß die Bürger – wenigstens in allgemeiner Form – über die Abgleichsverfahren unterrichtet werden und zu Feststellungen aus dem Abgleich gehört werden. In einer zentralen Vorschrift, die Grundlage für Datenabgleiche zur Mißbrauchsbekämpfung werden soll, sollte auch deren erfolgskontrollierende Begleitung verankert werden.

Leider ist das BMA auf meine Vorschläge inhaltlich nicht eingegangen. In einer eiligen Abstimmung zwischen den beteiligten Ressorts entstand der inzwischen verabschiedete § 67e SGB X, der die Befugnisse der Außenprüfungsgruppen von Bundesanstalt für Arbeit und Hauptzollämtern erweitert. Diese dürfen über den eigentlichen Kern ihrer Prüfaufgabe hinaus auch bestimmte sachverwandte Fragen aus dem Zuständigkeitsbereich anderer Sozialleistungsträger stellen und die Antworten an die für die Mißbrauchsbekämpfung insoweit zuständige Behörde weitergeben. Der rechtssystematisch wenig überzeugende Standort der neuen Vorschrift im Zweiten Kapitel SGB X erklärt sich aus dem ursprünglich weitergehenden Regelungsziel.

19.2 Der Münchner Sozialamtsfall und seine Folgen

Im Frühjahr 1997 hat der „Münchener Sozialamtsfall“ nicht nur bei den beteiligten Verwaltungen, sondern auch in Presse und Politik für Aufsehen gesorgt. Aufgrund einer Weisung des Leiters des Münchener Sozialamtes hatte dieses der Polizei Auskünfte über den nächsten Vorsprachetermin gesuchter Personen verweigert. Dies ist in der Öffentlichkeit heftig diskutiert worden. Dabei ist vielfach übersehen worden, daß schon nach geltendem Recht (§ 73 SGB X) zur Durchführung eines Strafverfahrens wegen eines Verbrechens eine inhaltlich sogar unbeschränkte Auskunft durch das Sozialamt zulässig ist; hierfür ist allerdings eine richterliche Anordnung erforderlich. Aber auch ohne eine solche Anordnung erlaubt § 68 SGB X eine Auskunft über die *„derzeitige Anschrift des Betroffenen“*, wobei es wegen einer Kammergerichtsentscheidung gängige Praxis der Verwaltung geworden ist, diese Übermittlungsbefugnis auch auf den derzeitigen Aufenthalt des Betroffenen, beispielsweise im Sozialamt, anzuwenden. Im Münchner Sozialamtsfall sollte die Auskunft aber über einen zukünftigen Termin im Sozialamt, also einen zukünftigen Aufenthalt gegeben werden und zwar ohne richterliche Anordnung. Das gab der insoweit eindeutige Wortlaut des Gesetzes nicht her. In meinen öffentlichen Stellungnahmen habe ich deutlich gemacht, daß ich gegen eine entsprechende Erweiterung der gesetzlichen Übermittlungsbefugnis keine Bedenken hätte.

Erst knapp ein Jahr später wurde ich an einem Entwurf zur Änderung von § 68 SGB X beteiligt, dann aber mit der Bitte um unverzügliche Zustimmung noch am gleichen Tag. Der Entwurf war jedoch auch innerhalb der Regierungskoalition nicht unumstritten; manchen ging er nicht weit genug. Infolge eines Mißverständnisses wurde dieser Entwurf nicht eingebracht. Der später Gesetz gewordene Wortlaut ist dann in der Regierungskoalition beschlossen worden. Im Rahmen meiner Beteiligung war es mir darauf angekommen, daß die Sozialämter aufgrund der Gesetzesänderung nicht zu einer Hilfsbehörde der Polizei werden, indem sie etwa regelrechte Fahndungsbücher anlegen und überwachen müßten. Die verabschiedete Vorschrift sieht als Einschränkung „im Einzelfall auf Ersuchen“ vor. Das mag zwar eher deklaratorische Bedeutung haben, da alle Übermittlungsbefugnisse der §§ 67f SGB X sich auf Übermittlungen im Einzelfall beziehen. Sie macht jedoch die Absicht des Gesetzgebers deutlich, daß mit der Ergänzung in § 68 SGB X kein Instrument für eine ständige Mitwirkung des Sozialamtes geschaffen werden sollte.

Die Änderung von § 68 SGB X ist erst im parlamentarischen Gang als Artikel 4 an das Medizinproduktegesetz angehängt worden. Dieses an sich nicht seltene Verfahren hat hier allerdings dazu geführt, daß der Ausschuß für Arbeit und Sozialordnung nicht beteiligt wurde. Die ablehnenden Stellungnahmen einiger Landesdatenschutzbeauftragter haben zu vereinzelten kritischen Äußerungen von Landesregierungen im Bundesrat geführt, die jedoch an seiner Zustimmung zu dem Gesetzentwurf im Ergebnis nichts geändert haben.

Die neue Fassung von § 68 SGB X ist auch nach ihrem Inkrafttreten in Fachkreisen kritisiert worden. Über eine „Aushöhlung des Sozialdatenschutzes“ als Folge der Ergänzung von § 68 SGB X ist viel spekuliert worden. Bei verantwortungsbewußter Handhabung – dazu zählen neben den bereits genannten Punkten die Berücksichtigung schutzwürdiger Interessen des Betroffenen und der Leitungsentscheidungsvorbehalt – halte ich sie hingegen weiter für datenschutzrechtlich vertretbar. Zur Verbreiterung der rechtstatsächlichen Basis auch im Hinblick auf zukünftige Fortentwicklungen des Sozialdatenschutzrechts habe ich die Verbände der meiner Beratungs- und Kontrollzuständigkeit unterliegenden Sozialleistungsträger gebeten, für die Dauer von einem halben Jahr die

tatsächliche Inanspruchnahme der geänderten Fassung von § 68 SGB X aufzuzeichnen. Nur wer weiß, wie sich eine Gesetzesänderung tatsächlich in der Praxis auswirkt, kann wirklich beurteilen, ob die Vorschrift ein vom Gesetzgeber angestrebtes Ziel erreicht, dahinter zurückbleibt oder darüber hinausschießt. Gerade in dem empfindlichen Rechtsbereich der Sozialgesetzgebung ist eine Art Rechtstatsachenforschung, wie sie im Strafrechtsbereich üblicher ist, von zunehmender Bedeutung. Sie trägt auch hier zur Versachlichung der Diskussion bei.

Eine andere Frage ist es, wie gut sich der geänderte § 68 SGB X in das Gefüge datenschutzrechtlicher Übermittlungsbefugnisse der §§ 68 bis 78 SGB X einpaßt. Unverkennbar sind Wertungswidersprüche geblieben, die mit Sicherheit den Ruf nach dem Gesetzgeber erneut laut werden lassen.

19.3 Sozialhilfedatenabgleichsverordnung

In 1993 war § 117 BSHG um eine Rechtsgrundlage für die Überprüfung der Berechtigung des Leistungsbezugs von Sozialhilfeempfängern im Wege von Datenabgleichen ergänzt worden. An dem Entwurf einer Rechtsverordnung über das Verfahren der Abgleiche hat mich das BMG 1997 beteiligt. Ich habe das BMG und den Verband Deutscher Rentenversicherungsträger (VDR) hierzu und bei der Verfahrenseinführung beraten.

Ziel der Überprüfung ist es, vom Sozialhilfeempfänger nicht angegebene Beschäftigungsverhältnisse oder konkurrierende Bezüge anderer Sozialleistungen aufzudekken. Dazu sollten dessen Daten mit den Daten

– der anderen Sozialämter,
– der Arbeitslosenversicherung,
– der Rentenversicherung,
– der Unfallversicherung,
– der Arbeitgeberdatei bei der Datenstelle der Rentenversicherungsträger und
– der Datei der geringfügigen Beschäftigungsverhältnisse, ebenfalls bei der vorstehend genannten Datenstelle

abgeglichen werden.

In diesen Abgleich sind auch Sozialdaten bundesunmittelbarer und landesunmittelbarer Leistungsträger einbezogen. Er kann sinnvoll nur über eine zentrale Vermittlungsstelle realisiert werden.

19.3.1 Kein Sozialdatenpool

Die Einrichtung einer Zentraldatei, eines sog. Sozialdatenpools, in der die Daten aller Sozialhilfeempfänger erfaßt wären und die Verknüpfungen auch mit anderen Dateien ermöglichte, hielte ich in Übereinstimmung mit dem BMJ für verfassungsrechtlich höchst problematisch. Im Rahmen meiner Beteiligung zur Sozialhilfedatenabgleichsverordnung habe ich daher auf eine Ausgestaltung des Verfahrens geachtet, die ohne fortdauernde zentrale Datenhaltung auskommt.

Der Abgleich erfolgt vierteljährlich für das zurückliegende Quartal. Er gliedert sich in vier jeweils zweiwöchige Phasen. In der **ersten Phase** werden die Daten von den teilnehmenden Sozialleistungsträgern (Anfragedatensätze) an die Vermittlungsstelle angeliefert; Träger der Vermittlungsstelle ist der VDR. In der **zweiten Phase** stellt die Vermittlungsstelle die angelieferten Daten für die im Gesetz festgelegten Auskunftsstellen zusammen und übermittelt sie an diese. Der eigentliche Abgleich erfolgt bei den Auskunftsstellen in der **dritten Phase**. Die hieraus resultierenden Rückmeldungen werden unmittelbar in gesonderte Ergebnisdateien für die teilnehmenden Sozialhilfeträger aufgeteilt, aus denen sie in der **vierten Phase** von den Sozialhilfeträgern abgefragt werden können.

Nach dem Verfahrensablauf liegt bei der Vermittlungsstelle ein Gesamtbestand der von den teilnehmenden Sozialhilfeträgern gemeldeten Sozialhilfeempfänger nur in der zweiten Phase für die Dauer von längstens zwei Wochen (alle drei Monate) vor. Schon hierzu sind während der Ressortabstimmung verfassungsrechtliche Bedenken laut geworden. Nach meiner Auffassung kann diese kurzfristige Speicherung zum Zweck der Vermittlung jedoch hingenommen werden, wenn der Zeitraum der Speicherung des Gesamtbestandes so kurz wie möglich gehalten wird.

19.3.2 Keine falschen Schlüsse ziehen!

Das Abgleichverfahren meldet den teilnehmenden Sozialhilfeträgern alle festgestellten parallelen Leistungsbezüge und Beschäftigungsverhältnisse im zurückliegenden Abgleichszeitraum (3 Monate). Hier kann es zu Meldungen kommen, die eigentlich keinen Verdacht eines unrechtmäßigen oder mißbräuchlichen Sozialhilfebezugs begründen. Insbesondere folgende Konstellationen – eines rechtmäßigen Sozialhilfebezugs – werden hierzu leider systembedingt zurückgemeldet:

– Als Ergebnis des Abgleichs werden auch die Leistungsbezüge und Beschäftigungsverhältnisse gemeldet, die der Sozialhilfeempfänger ordungsgemäß angegeben hat. Das gilt beispielsweise für denjenigen, der eine geringe Arbeitslosenhilfe bezieht oder einer geringfügigen Beschäftigung nachgeht und eben ergänzend Sozialhlfe bezieht.
– Auch Änderungen der bei der Berechnung der Sozialhilfe berücksichtigten Lebensverhältnisse des Sozialhilfeempfängers innerhalb des dreimonatigen Abgleichszeitraums können eine Rückmeldung bewirken. Bezog jemand beispielsweise nur im Januar Sozialhilfe, nahm ab Februar wieder eine Arbeit auf und hat die Arbeitsaufnahme ordnungsgemäß angezeigt und der Sozialhilfebezug wurde ab Februar eingestellt, so wird gleichwohl zu ihm ein Ergebnis, ein Treffer, zurückgemeldet. Entsprechendes gilt, wenn der Betroffene beispielsweise bis Ende Juli Arbeitslosenhilfe bezog und ab August Sozialhilfe.
– Als wesentliche Fehlerquelle der Ergebnisse des Abgleichs hat sich die Datei der geringfügig Beschäftigten (§ 105 Abs. 3 SGB IV) herausgestellt. Die in ihr gespeicherten Angaben beruhen praktisch ausschließ-

lich auf den gesetzlich vorgeschriebenen An- und Abmeldungen der Arbeitgeber der geringfügigen Beschäftigungsverhältnisse. Versäumt der Arbeitgeber die Abmeldung bei Beendigung des geringfügigen Beschäftigungsverhältnisses, so bleibt der Arbeitnehmer zu Unrecht als „beschäftigt“ registriert. Ein solches Versäumnis des Arbeitgebers kann unter Umständen jahrelang unbemerkt bleiben, weil sich an den Eintrag keine unmittelbaren Rechtsfolgen für die Beteiligten knüpfen. Die Datei dient nämlich lediglich dem Aufdecken mehrfacher Beschäftigungsverhältnisse unter Überschreitung der Zeitgrenzen für geringfügige Beschäftigungsverhältnisse und mehreren weiteren Kontrollverfahren, zu denen auch der Sozialhilfedatenabgleich zählt. Sie gilt daher auch in Fachkreisen als fehlerträchtig. Eine Rückmeldung, die auf dem Abgleich mit dieser Datei beruht, begründet daher noch keinen hinreichenden Verdacht eines Mißbrauchs (s. auch oben erster Spiegelstrich).

Schon diese drei wesentlichsten Fallkonstellationen machen deutlich, daß die aus dem automatisierten Sozialhilfedatenabgleich hervorgehenden „Treffer“ keinesfalls bereits als Verdachtsfälle bezeichnet werden dürfen. Es ist daher unverzichtbar, zu allen Rückmeldungen zunächst in der Akte des Sozialhilfeträgers zu überprüfen, ob der Sozialhilfeempfänger die entsprechenden Angaben nicht bereits selbst gemacht hatte. Verbleibt danach Aufklärungsbedarf, so muß zunächst dem Sozialhilfeempfänger nach Maßgabe des sog. Ersterhebungsgrundsatzes selbst Gelegenheit zur Äußerung gegeben werden. Das gilt besonders für alle Rückmeldungen, die auf dem Abgleich mit der Datei der geringfügig Beschäftigten beruhen. Würde der Sozialhilfeträger – davon abweichend – den Arbeitgeber des z. B. Jahre zuvor beendeten geringfügigen Beschäftigungsverhältnisses befragen, so würde diesem durch die Anfrage des Sozialamtes signalisiert, daß sein früherer Arbeitnehmer jetzt Sozialhilfe bezieht und daß das Sozialamt wegen Unregelmäßigkeiten ermittelt. Sozialhilfeempfänger könnten so – ohne Grund – in Mißkredit geraten.

Die richtige und sachgerechte Bewertung und Nutzung der Ergebnisse des Sozialhilfedatenabgleichs bei den Sozialhilfeträgern erfordert also ein genaues Verständnis des Verfahrens.

Die genannten Zusammenhänge insbesondere im Hinblick auf den Abgleich mit der Datei der geringfügig Beschäftigten habe ich in einem Schreiben an das BMG, den VDR und die Landesbeauftragten für den Datenschutz eingehend dargestellt. Der VDR als Träger der Vermittlungsstelle hat dieses Schreiben seinem verfahrenseinführenden Schreiben an die Sozialhilfeträger und die Auskunftsstellen beigefügt.

Da die Sozialhilfeträger kommunale Stellen sind, liegt die datenschutzrechtlche Begleitung und Kontrolle der praktischen Durchführung des Sozialhilfedatenabgleichsverfahrens bei den Landesbeauftragten für den Datenschutz. Aus dem Erfahrungsaustausch mit ihnen ist mir bekannt, daß die nach den beschriebenen konzeptionsbedingten Besonderheiten zu erwartenden Probleme in der Praxis tatsächlich auftreten. Es gilt vor allem zu vermeiden, daß ein Sozialhilfeempfänger, der durch eine geringfügige Beschäftigung zu seinem Lebensunterhalt selbst beiträgt, zu Unrecht des Mißbrauchs verdächtigt wird, weil das Verfahren, mit dem seine Angaben überprüft werden, auf eine nicht korrekte Datei zurückgreift. Die notwendige Schulung und Information der Empfänger der Rückmeldungen sollte nicht nur ein datenschutzrechtliches, sondern auch ein sozialpolitisches Anliegen sein.

19.3.3 Erfolgskontrollierende wissenschaftliche Begleitung

Im Vorfeld der Realisierung des Sozialhilfedatenabgleichs war eine lebhafte öffentliche Diskussion darüber geführt worden, wie hoch die Mißbrauchsquote unter den Sozialhilfeempfängern sei. Die breite Spanne der Diskussion hat deutlich gemacht, daß tragfähige Erkenntnisse über Umfang und Struktur mißbräuchlicher Inanspruchnahme von Sozialleistungen nicht vorlagen. Auf meine Anregung hat das BMG eine Untersuchung zur wissenschaftlichen Begleitung der Einführung des Sozialhilfedatenabgleichs bei dem Institut für Sozialforschung und Gesellschaftspolitik (ISG) in Auftrag gegeben. Dabei geht es nicht einfach nur darum, die bloße Prozentzahl festgestellten unrechtmäßigen Leistungsbezugs zu ermitteln, sondern vor allem darum, qualitative Aussagen zu gewinnen. Wenn bekannt ist, welche falschen Angaben zu unrechtmäßigem Leistungsbezug führen, sollten gezielte Fragen bei der Antragstellung von vornherein vorgesehen werden. Zu den wesentlichen Aspekten, zu denen ich mir Aufschluß durch die Begleitforschung erwarte, gehören die dem Abgleich zugeschriebene präventive Wirkung, weil die Betroffenen hierauf hingewiesen werden, aber auch die Frage, welche regionalen Unterschiede etwa zwischen städtischen und ländlichen Bereichen bestehen. So wird vermutet, daß eine stärkere gegenseitige Sozialkontrolle auf dem Land dem Mißbrauch entgegenwirkt.

Der Sachstandsbericht des ISG nach dem ersten Datenabgleich bestätigt, daß nur bei einem Teil der durch den Abgleich aufgezeigten Rückmeldungen tatsächlich unrechtmäßiger Sozialhilfebezug vorliegt. Der Bericht ist nicht veröffentlicht.

19.4 Änderung datenschutzrechtlicher Zuständigkeiten für Sozialleistungsträger

Die auf der Grundlage eines in Artikel 5 des Einigungsvertrages enthaltenen Auftrages eingerichtete Gemeinsame Verfassungskommission von Bundestag und Bundesrat hatte einen Bericht mit Empfehlungen für Grundgesetzänderungen vorgelegt, um die *„im Zusammenhang mit der deutschen Einigung aufgeworfenen Fragen“* angemessenen Lösungen zuzuführen. Eine Folge war die Ergänzung von Artikel 87 Abs. 2 GG.

Nach Artikel 87 Abs. 2 GG alte Fassung wurden diejenigen sozialen Versicherungsträger als bundesunmittelbare Körperschaft geführt, *„deren Zuständigkeitsbereich sich über das Gebiet eines Landes hinaus ersteckt.“* Nach dem Ende 1994 neu angefügten Satz 2 bleibt ein sozialer

Versicherungsträger, dessen Zuständigkeitsbereich sich auf bis zu drei Bundesländer erstreckt, eine landesunmittelbare Körperschaft des öffentlichen Rechts, wenn die beteiligten Länder das aufsichtführende Land einvernehmlich bestimmt haben. Solange eine solche Bestimmung nicht erfolgt ist und bei den Sozialversicherungsträgern, deren Zuständigkeitsbereich sich auf vier oder mehr Länder erstreckt, bleibt es hingegen bei deren Bundesunmittelbarkeit. Der zu Artikel 87 Satz 2 GG zwischen allen Bundesländern geschlossene Staatsvertrag ist nach Ratifizierung und Hinterlegung am 1. Juni 1997 in Kraft getreten. Nach ihm kommt die Aufsicht grundsätzlich dem Land zu, in dem der Versicherungsträger seinen Sitz hat. Die Rechtsänderung hat über § 81 Abs. 2 SGB X entsprechende Bedeutung für die Zuständigkeit bei der Datenschutzkontrolle.

Praktische Auswirkungen entfaltet sie vor allem für Betriebs- und Innungskrankenkassen entsprechender Größe. Bei ihnen kommt es jeweils im Einzelfall darauf an, auf wieviele Bundesländer sich ihr Einzugsbereich erstreckt. Wenn sich Bürger mit einem datenschutzrechtlichen Anliegen an mich wenden, kann daher allein zur Klärung dieser Vorfrage eine Korrespondenz mit der Krankenkasse erforderlich sein. Dies kann von den Bürgern als bürokratisch empfunden werden. Ich gehe jedoch davon aus, daß derartige Fälle selten vorkommen.

Meine bisherige Zuständigkeit für die Landesversicherungsanstalt Oldenburg-Bremen ist infolge der Änderung von Artikel 87 Abs. 2 GG auf den Landesbeauftragten für den Datenschutz Niedersachsen übergegangen. Soweit die Landesversicherungsanstalt Oldenburg-Bremen Aufgaben nach dem Künstlersozialversicherungsgesetz wahrnimmt, bleibt es jedoch bei meiner Zuständigkeit.

19.5 Gesundheitswesen Wismut

Das umfangreiche Gesundheitsdatenarchiv des ehemaligen Uranerzbergbaus „SDAG Wismut“ (Sowjetisch-Deutsche Aktiengesellschaft Wismut) ist einerseits von erheblicher Bedeutung für die medizinische und berufsgenossenschaftliche Betreuung ehemaliger Mitarbeiter und bietet andererseits die einzigartige Möglichkeit wissenschaftlicher Erforschung von Risiken und Folgen der Uranexposition. Über die gesetzliche Regelung für die Behandlung dieses Datenbestandes habe ich bereits berichtet (14. TB Nr. 2.4, 16. TB Nr. 19.4).

Das Gesetz hat das Gesundheitsdatenarchiv auf die Bundesanstalt für Arbeitsschutz und Arbeitsmedizin (BAfAM) übertragen. Einige Einrichtungen des Gesundheitswesens Wismut werden heute als Krankenhäuser in privater Trägerschaft fortgeführt. Nach dem Wortlaut des Gesetzes sind auch die dort verbliebenen Patientenunterlagen auf die BAfAM übergegangen. Die BAfAM hat deshalb gegenüber den betroffenen Krankenhäusern ihren Rechtsanspruch auf diese Altakten geltend gemacht. Dieses Schreiben hat bei den Krankenhäusern für Unruhe gesorgt, zumal einige der Patienten weiter von ihnen medizinisch betreut wurden. Die Behinderung der Behandlung von Patienten wäre eine Folge, die mit den Absichten des Gesetzgebers keinesfalls vereinbar wäre. Die BAfAM hat die Verfolgung ihres formalrechtlichen Herausgabeanspruchs ausgesetzt. Hinsichtlich abgeschlossener Patientenunterlagen, beispielsweise von verstorbenen früheren Mitarbeitern der SDAG Wismut, bedeutet dies eine erhebliche Verlängerung der Aufbewahrungsfristen, so daß einige Krankenhäuser diese Akten aus Kapazitätsgründen gern abgeben würden. Ich stehe mit der BAfAM in Kontakt, um eine angemessene Lösung zu finden.

19.6 Postmortaler Sozialdatenschutz

Schon oft bin ich zu Umfang und Grenzen des Sozialdatenschutzes von Verstorbenen gefragt worden. Beispielsweise kann es im Interesse des Erben liegen, von der Krankenkasse des Verstorbenen Auskünfte über Behandlungsdaten zu erhalten, um sie gegenüber einer Lebensversicherung oder in einer Erbauseinandersetzung zu verwenden.

Anliegen des Datenschutzes ist es, den Umgang mit personenbezogenen Daten zu regeln und das sind *„Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person“* (§ 3 Abs. 1 BDSG, ebenso § 67 Abs. 1 SGB X), also eines lebenden Menschen.

Die Daten Verstorbener werden auch in der EU-Datenschutzrichtlinie (s. o. Nr. 2.1) nicht angesprochen. Rat und Kommission stimmen darin überein, daß es den Mitgliedstaaten überlassen bleibt, über das Ob und den Umfang der Einbeziehung der Daten Verstorbener in das innerstaatliche Recht zu entscheiden. Verstorbene unterliegen auch nicht dem Schutz des allgemeinen Persönlichkeitsrechts, da dieses mit dem Tode erlischt. Dagegen ist die Würde des Menschen nach Artikel 1 Abs. 1 GG auch nach seinem Tode zu respektieren. Auch gelten einzelne Berufs- oder besondere Amtsgeheimnisse, wie Arzt-, Statistik- und Steuergeheimnis, zeitlich über den Tod des Betroffenen hinaus, wobei jedoch die Schutzintensität mit der Zeit abnimmt.

Die Anwendbarkeit sozialdatenschutzrechtlicher Vorschriften ist hingegen durch § 35 Abs. 5 SGB I auch auf die Zeit nach dem Tod des Betroffenen ausgedehnt. Nach § 35 Abs. 5 Satz 1 SGB I dürfen Sozialdaten Verstorbener nach Maßgabe des Zweiten Kapitels des SGB X verarbeitet oder genutzt werden. Eine gesetzliche Übermittlungsbefugnis an Angehörige, wie sie nach § 67d Abs. 1 SGB X erforderlich wäre, kann für diesen Fall weder den §§ 68 bis 77 SGB X noch einer anderen Rechtsvorschrift des SGB entnommen werden. Meines Erachtens kann ein Auskunftsanspruch für Angehörige auch nicht in analoger Anwendung von § 83 SGB X abgeleitet werden; der eindeutig die Auskunft nur an den Betroffenen regelt.

Folglich kommt für die Weitergabe von Sozialdaten Verstorbener an deren Angehörige nur § 35 Abs. 5 Satz 2 SGB I in Betracht. Danach dürfen die Daten außerdem verarbeitet und genutzt werden, *„wenn schutzwürdige Interessen des Verstorbenen oder seiner Angehörigen dadurch nicht beeinträchtigt werden können“*. Es kommt also neben den schutzwürdigen Interessen des Verstor-

benen auf die seiner Angehörigen an, nicht auf die der bürgerlich-rechtlichen Erben. Der Begriff der Angehörigen dürfte nach Sinn und Zweck der Vorschrift in Anlehnung an § 56 Abs. 1 Nr. 1 bis 3, Abs. 2 und 3 SGB I auszulegen sein. Die schutzwürdigen Interessen sind in objektiver Beurteilung zu bestimmen. Dabei kommt es darauf an, welchen Zweck die Angehörigen mit der Kenntnis der Sozialdaten verfolgen (Klärung von Rechtsbeziehungen, Abwicklung von Ansprüchen). In diesem Zusammenhang kann die Anhörung von Angehörigen im Einzelfall hilfreich oder geboten sein, um den Grund des Auskunftsersuchens zu ermitteln.

Nach dem Wortlaut von § 35 Abs. 5 Satz 2 SGB I können Sozialdaten dann übermittelt werden, wenn schutzwürdige Interessen *„nicht beeinträchtigt werden können“*. Im Ergebnis heißt das, daß ein Sozialleistungsträger Sozialdaten Verstorbener weitergeben darf. Er hat jedoch gesetzliche Schranken zu beachten, die vor allem bei der Weitergabe an einzelne Personen eine Auseinandersetzung mit den Gründen für die Anfrage, der Familie des Verstorbenen und dem Fall des Verstorbenen selbst erfordert.

19.7 Begutachtung in Anwesenheit einer Begleitperson

Durch eine Eingabe mußte ich mich mit der interessanten Frage auseinandersetzen, ob es rechtmäßig ist, seitens der BfA die Hinzuziehung einer Begleitperson bei der Durchführung einer ärztlichen Begutachtung oder Untersuchung zu verweigern.

In dem zugrundeliegenden Fall hatte die BfA die Auffassung vertreten, daß eine vorgesehene Begutachtung nur ohne Beiziehung einer Begleitperson erfolgen kann.

Ich habe diesen Einzelfall mit der BfA besprochen und bin mit ihr zu dem Ergebnis gelangt, daß jeder Versicherte grundsätzlich das Recht hat, zu einer ärztlichen Begutachtung oder Untersuchung eine Begleitperson als Zeugen oder als persönlichen Beistand beizuziehen. Dies schließt nicht aus, daß in Ausnahmefällen überwiegende medizinische Gründe gegen eine ständig anwesende Begleitperson sprechen.

Dieses Ergebnis, das für den gesamten Bereich der Sozialverwaltung Bedeutung hat, entspricht auch dem ärztlichen Standesrecht, wonach die Hinzuziehung Dritter der Zustimmung des Patienten und des Arztes bedarf.

19.8 Verbesserter Datenaustausch bei Sozialleistungen

Die Konferenz der Arbeits- und Sozialminister (ASMK) hatte 1995 eine Arbeitsgruppe unter Vorsitz des Freistaates Bayerns eingesetzt mit dem Auftrag zu untersuchen, ob der Datenaustausch bei Sozialleistungen verbessert werden kann. Im Juli 1997 hat mir die Arbeitsgruppe den umfangreichen Entwurf ihres Berichts mit der Bitte um Stellungnahme innerhalb eines Monats zugeleitet. Der Entwurf enthielt eine Vielzahl von Vorschlägen sowohl an den Gesetzgeber als auch für den Verwaltungsvollzug. Da sie sich auf alle Sozialleistungsbereiche bezogen und damit praktische Bedeutung auch für die Sozialleistungsträger im Zuständigkeitsbereich der Landesbeauftragten für den Datenschutz hatten, habe ich meine Stellungnahme gemeinsam mit ihnen erarbeitet. Besonders anzumerken ist, daß die Vorschläge der Arbeitsgruppe in mehreren Punkten das vom Gesetzgeber entwickelte System der Differenzierung des Erhebungsverfahrens im Sozialdatenschutz aufgeben. Die Datenschutzbeauftragten des Bundes und der Länder haben sich mit den Vorschlägen der Arbeitsgruppe der ASMK „Verbesserter Datenaustausch bei Sozialleistungen“ auseinandergesetzt und ihre Beratung angeboten (s. hierzu **Anlage 12**). In ihrer 74. Sitzung Ende Oktober 1997 hat die ASMK beschlossen, die Bundesregierung zu bitten, *„die erforderlichen Schritte zur Realisierung eines verbesserten Datenaustauschs in diesem Sinne in die Wege zu leiten, dabei unter Einschluß des Gesprächsangebotes der Datenschutzbeauftragten den Bericht der Arbeitsgruppe und die Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 23./24. Oktober 1997 in die Prüfung einzubeziehen und der ASMK bis zum nächsten Jahr zu berichten.“*

Das Gesprächsangebot ist bisher nicht aufgegriffen worden. Allerdings hat der Freistaat Bayern im Bundesrat einen Gesetzantrag „Entwurf eines Gesetzes zur Schaffung von Arbeitsanreizen und zur Vermeidung von Mißbrauch in der Sozialhilfe“ eingebracht (BR-Drucksache 388/ 98 vom 29. April 1998), in dem einige der von der ASMK-Arbeitsgruppe gegenüber dem Gesetzgeber unterbreiteten Vorschläge enthalten sind. Die mit der Angelegenheit befaßten Ausschüsse des Bundesrates haben das Ruhen dieses Antrages beschlossen, bis Bayern diesen wieder aufgreift.

19.9 Neuordnung der Sozialmedizinischen Begutachtung

Leistungen der Sozialversicherungsträger werden in vielen Fällen erst nach gutachterlicher ärztlicher Stellungnahme gewährt. Das ärztliche Gutachten ist damit regelmäßig das Herzstück dieser Verfahren. Der eminenten Bedeutung stehen allerdings für den Versicherten oftmals nicht durchschaubare Rahmenbedingungen gegenüber:

Es existieren vielfältige sozialmedizinische Zuständigkeiten, wie der Medizinische Dienst der Krankenversicherung, der Arbeitsamtsarzt, der Sozialmedizinische Dienst der Rentenversicherung, die beratenden Ärzte der Berufsgenossenschaften, das Gesundheitsamt sowie externe Gutachter. Diese Vielfalt führt zu unterschiedlichen Graden finanzieller und/oder beruflicher Verflechtung zwischen Kostenträger und ärztlichem Gutachter. Zudem können aus eventuell durchgeführten Doppeluntersuchungen widersprüchliche Urteile resultieren.

Vor diesem Hintergrund ist die Einrichtung regionaler Sozialmedizinischer Zentren diskutiert worden (vgl. im einzelnen BT-Drs. 13/6587), deren Zielsetzung darin besteht, eine größere Unabhängikeit der Begutachtenden sowie stimmige und verbindliche Bewertungsmaßstäbe sicherzustellen und darüber hinaus belastende Doppeluntersuchungen zu vermeiden.

Aus Datenschutzsicht sind hier zwei Fragestellungen von besonderer Bedeutung:

– Nach § 96 Abs. 3 SGB X ist die Bildung einer Zentraldatei mehrerer Leistungsträger für Daten der ärztlich untersuchten Leistungsempfänger grundsätzlich unzulässig. Diese Regelung soll sicherstellen, daß die nach § 96 Abs. 1 und Abs. 2 SGB X vorgesehene Zusammenarbeit der Leistungsträger nicht zur Bildung einer medizinischen Zentraldatenbank von mehreren Trägern führt.

  Nach meiner Auffassung steht die Regelung des § 96 Abs. 3 SGB der Einrichtung Sozialmedizinischer Zentren aber nicht von vornherein entgegen. Denkbar wäre eine den § 276 Abs. 2 Satz 6 SGB V, § 97 Abs. 3 Satz 3 SGB XI entsprechende Lösung. Nach diesen Vorschriften darf der Medizinische Dienst in Dateien nur Angaben zur Person und Hinweise auf bei ihm vorhandene Akten aufnehmen. Ein anderer Weg könnte eine nach Leistungsträgern getrennte Konzeption sein, wobei durch technische und organisatorische Maßnahmen sicherzustellen ist, daß Versichertendaten der einzelnen Leistungsträger nicht zusammengeführt werden können.

– Das durch die Einrichtung Sozialmedizinischer Zentren beabsichtigte Ziel, eine größere Unabhängigkeit der Begutachtenden zu gewährleisten sowie Zuständigkeiten zu entwirren, begrüße ich besonders, da es vor allem geeignet ist, die Transparenz für den Versicherten zu erhöhen und so auch zur Akzeptanz der Entscheidungen beizutragen. Bereits im Gesetzgebungsverfahren zum Sozialgesetzbuch – Gesetzliche Unfallversicherung (SGB VII) – war ich mit der Frage nach der Unabhängigkeit externer Gutachter befaßt. Im Ergebnis führte die Diskussion zu dieser Frage zur Regelung des § 200 Abs. 2 SGB VII, wonach der Unfallversicherungsträger vor Erteilung des Gutachtenauftrages dem Versicherten mehrere Gutachter zur Auswahl benennen soll; zudem sieht diese Regelung vor, daß der Versicherte der Übermittlung seiner Daten an einen externen Gutachter widersprechen kann (vgl. im einzelnen Nr. 23.4).

20 Arbeitsverwaltung

20.1 Ansprechpartner für Datenschutzangelegenheiten

Im Zusammenhang mit der Wahrnehmung der Aufgaben des Datenschutzbeauftragten der Bundesanstalt für Arbeit (BA) habe ich dem Ausschuß für Arbeit und Sozialordnung des Deutschen Bundestages erläutert, daß der Datenschutz in den Arbeitsämtern verbessert werden könnte (Drucksache 13/5936, S. 25). Kunden der Arbeitsämter – so werden die Bürger bezeichnet, die Leistungen des Arbeitsamtes in Anspruch nehmen – hatten bislang nicht die Möglichkeit, sich unabhängig von der fachlichen Betreuung durch den zuständigen Sachbearbeiter von einem besonders ausgebildeten Mitarbeiter des Arbeitsamtes datenschutzrechtlich beraten zu lassen.

Daraufhin habe ich dieses Thema mit der BA eingehend diskutiert. Mit ihrem Runderlaß 46/97 vom 10. September 1997 hat sie mit sofortiger Wirkung festgelegt, daß in den Arbeitsämtern Ansprechpartner für Datenschutzangelegenheiten der Kunden zu benennen sind. Vorzusehen sind dafür mindestens zwei Abschnittsleiter, die – neben ihren originären Aufgaben – für den Kontakt zu Kunden in datenschutzrechtlichen Fragen oder wegen Beschwerden zuständig sind. In den Nebenstellen wurden deren Leiter als Ansprechpartner benannt. Die BA hat in dem Runderlaß bestätigt, daß die neue Aufgabe *„sowohl der Kundenorientierung, der Effizienz und Effektivität als auch dem Anliegen des fachintegrierten Datenschutzes“* entspricht.

Zwischenzeitlich konnte ich feststellen, daß der Runderlaß umgesetzt ist. Die künftigen Erfahrungen mit den genannten Ansprechpartnern werden zeigen, ob und wie die gemeinsam gefundene Lösung sich bewähren wird.

20.2 Datenabgleich bei Freistellungsaufträgen von Arbeitslosenhilfeempfängern

In meinem 16. TB (Nr. 7.10) hatte ich auf die mit dem Jahressteuergesetz 1997 neu eingeführte Regelung für einen Datenabgleich zur Bekämpfung von Leistungsmißbrauch bei dem Bezug von Arbeitslosenhilfe hingewiesen:

Nach § 45d Abs. 3 Einkommensteuergesetz (EStG) darf das Bundesamt für Finanzen (BfF) der BA auf deren Ersuchen die *„Anzahl“* der von einem Leistungsbezieher erteilten Freistellungsaufträge zur Überprüfung des bei der Arbeitslosenhilfe zu berücksichtigenden Vermögens mitteilen. Nachdem inzwischen Erfahrungen der Praxis vorliegen, läßt sich nunmehr bewerten, ob das damit ermöglichte Datenabgleichsverfahren auch erforderlich und verhältnismäßig ist.

Auszugehen ist davon, daß arbeitslose Arbeitnehmer nach § 190 Abs. 1 Nr. 5 SGB III nur Anspruch auf Arbeitslosenhilfe haben, wenn sie – neben anderen Voraussetzungen – *„bedürftig“* sind. Ein Arbeitsloser ist u. a. nicht bedürftig, *„solange mit Rücksicht auf sein Vermögen, das Vermögen seines nicht dauernd getrennt lebenden Ehegatten oder das Vermögen einer Person, die mit dem Arbeitslosen in eheähnlicher Gemeinschaft lebt, die Erbringung von Arbeitslosenhilfe nicht gerechtfertigt ist“* (§ 193 Abs. 2 SGB III). Das Arbeitsamt hat die entsprechenden Angaben des Antragstellers zu überprüfen; es kann diese auch nachträglich kontrollieren. Hierfür hat der Antragsteller in dem Zusatzblatt „Bedürftigkeitsprüfung“ zu seinem Antrag auf Arbeitslosenhilfe die Anzahl seiner Freistellungsaufträge einzutragen.

Diese Angabe bildet zusammen mit der Mitteilung des BfF an die BA zur Anzahl der Freistellungsaufträge die Grundlage für die Ermittlungen der Arbeitsämter über die Vermögensverhältnisse der Antragsteller bzw. Leistungsempfänger. Wenn die vom BfF mitgeteilte Anzahl höher ist als die von einem Antragsteller angegebene, wird er gebeten, die betroffenen Institute, z. B. Banken, zu benennen sowie das jeweilige Guthaben nachzuweisen.

Soweit es dem Antragsteller oder Leistungsempfänger nicht möglich war, die Institute zu benennen, erhielt er bei

einer Anfrage beim BfF – zu Unrecht (s. o. Nr. 7.1) – zunächst zwar selbst keine Auskunft. Diese bekam nur das Arbeitsamt, wenn es mit Einwilligung des Betroffenen beim BfF nachfragte. Wenn es die Sachaufklärung erfordert, kann das Arbeitsamt je nach den Umständen des Sachverhalts nach entsprechender Kenntnis aber auch von den Instituten Auskünfte, beispielsweise über den Kontostand, verlangen (§ 315 Abs. 2 und 5 SGB III).

Im September 1997 wurde vom Zentralamt der BA eine erste automatisierte Anfrage wegen ca. 200 000 laufender Fälle an das BfF gerichtet. Zur Zeit wird grundsätzlich wegen derjenigen Leistungsfälle beim BfF angefragt, bei denen in Kürze der Bewilligungszeitraum ausläuft und eine Anfrage noch nicht durchgeführt worden ist. Die Arbeitsämter werden vom Zentralamt der BA über die Auskünfte des BfF unterrichtet, soweit darin mindestens ein Freistellungsauftrag als beim BfF gespeichert angegeben wird.

Nach Auskünften des BMA und den Ausführungen der Bundesregierung in ihrer Antwort auf eine Kleine Anfrage (Drucksache 13/11418, dort Antworten auf die Fragen 7ff.) hat der Datenabgleich für die Zeit von September 1997 bis zum 30. Juni 1998 folgende Ergebnisse erbracht:

Zu 911 813 Anfragen der Arbeitsämter waren insgesamt in 331 602 Fällen Freistellungsaufträge gespeichert. Hiervon waren bis Ende Juni 1998 Auskünfte des BfF zu 257 110 Betroffenen ausgewertet. In 177 406 Fällen machte dies Nachfragen erforderlich, weil die im Zusatzblatt „Bedürftigkeitsprüfung" zum Antrag auf Arbeitslosenhilfe angegebene Zahl der Freistellungsaufträge mit der vom BfF mitgeteilten Zahl nicht übereinstimmte. Aufgrund dieser Nachfragen haben 316 Betroffene ihren Antrag auf Arbeitslosenhilfe zurückgezogen und in 6 482 Fällen wurden Bewilligungsbescheide als rechtswidrig oder wegen Änderung der Verhältnisse nach den §§ 45 oder 48 SGB X aufgehoben. In weiteren 4 309 Fällen wurde die Arbeitslosenhilfe nach § 60 i.V.m. § 66 SGB I entzogen oder versagt, weil der Betroffene an der Aufklärung der unterschiedlichen Angaben zu den Freistellungsaufträgen nicht mitgewirkt hatte.

Ausgehend von der Dauer des Wegfalls der Bedürftigkeit wegen doch vorhandenen Vermögens und dem durchschnittlichen wöchentlichen Leistungssatz an Arbeitslosenhilfe zum 31. Dezember 1997 bzw. zum 30. Juni 1998 ergaben sich aufgrund der 6 482 Aufhebungsfälle insgesamt – unter Einschluß der eingesparten Sozialversicherungsbeiträge – Einsparungen in Höhe von 84,7 Mio. DM.

Unter der Voraussetzung, daß bei den zurückgezogenen Anträgen und der Zahl der abschließenden Entscheidungen nach § 60 i.V.m. § 66 SGB I (4 309 Fälle) für die Dauer des Wegfalls der Bedürftigkeit und des durchschnittlichen Leistungssatzes die gleichen Verhältnisse gelten wie bei den Aufhebungsentscheidungen geht die Bundesregierung von einer weiteren Ersparnis für denselben Zeitraum von 63,2 Mio. DM aus.

Das möglicherweise zusätzliche Einsparvolumen, das sich daraus ergibt, daß im Hinblick auf die Vermögensüberprüfung Anträge erst gar nicht gestellt wurden, läßt sich nicht einschätzen. Auch läßt sich nicht feststellen, ob und inwieweit die Überprüfungsmaßnahmen bei den Antragstellern zu korrekteren Angaben über das Vermögen geführt haben.

Seit Ende September 1998 sind die meisten, die langfristig Arbeitslosenhilfe beziehen, überprüft und ab Oktober 1998 wird im wesentlichen lediglich wegen der seit Einführung der maschinellen Anfrage angefallenen Neufälle beim BfF angefragt. Das Ergebnis der Einsparungen dürfte daher für die zweite Jahreshälfte 1998 und die Folgezeit geringer ausfallen.

Angesichts der aufgezeigten Ergebnisse kann ich mich der Notwendigkeit dieses Datenabgleichs nicht verschließen. Der Gesetzgeber hat mit den §§ 190 Abs. 1 Nr. 5, 193 Abs. 2 SGB III festgelegt, daß die für die Arbeitslosenhilfe aufzuwendenden Steuergelder nur geleistet werden dürfen, wenn der Betroffene u. a. kein Vermögen zur Verfügung hat und daher bedürftig ist. Dies bringt zwangsläufig mit sich, daß die Bedürftigkeit des Arbeitslosen zu überprüfen ist.

Das Grundgesetz hat, wie u. a. das Volkszählungsurteil des Bundesverfassungsgerichts ausführt, das Spannungsverhältnis zwischen Individuum und Gemeinschaft im Sinne der Gemeinschaftsbezogenheit der Person entschieden (BVerfGE 65, 1, 44). Der Einzelne muß grundsätzlich Einschränkungen seines Rechts auf informationelle Selbstbestimmung im überwiegenden Allgemeininteresse hinnnehmen (aaO). Die Zahl der im beschriebenen Zeitraum von einem Dreivierteljahr festgestellten Leistungsempfänger, die wegen vorhandenen Vermögens nicht bedürftig sind (siehe zumindest die 6 482 Aufhebungsentscheidungen), ist zwar im Verhältnis zu der Zahl der Leistungsempfänger, über die beim BfF wegen der Anzahl der dort gespeicherten Freistellungsaufträge nachgefragt wurde (911 813 Anfragen), nicht sonderlich hoch. Angesichts der von den Arbeitsämtern ermittelten beträchtlichen Einsparungen und der sicher auch bestehenden Präventivwirkung des Verfahrens sehe ich derzeit aber ein überwiegendes Allgemeininteresse an dem Datenabgleich als Voraussetzung der Vermögensüberprüfungen als gegeben an. In Zukunft wird zu beobachten sein, ob die Feststellungen es weiter rechtfertigen, den Datenabgleich zur Erreichung des in den §§ 190 Abs. 1 Nr. 5, 193 Abs. 2 SGB III festgelegten Zieles als erforderlich und auch verhältnismäßig anzusehen. Ich halte es aber auch für notwendig, die Rechtsgrundlage für die Abfragen der BA beim BfF in § 45d Abs. 3 EStG zu verbessern werden und entsprechend der Praxis deutlich zum Ausdruck zu bringen, daß ein automatisierter Datenabgleich zugelassen ist.

20.3 Nachweis fehlender Bedürftigkeit, wenn keine Zahlung von Arbeitslosenhilfe beantragt wird?

Mehrere Bürger, die sich beim Arbeitsamt arbeitslos gemeldet hatten, haben sich an mich gewandt, weil sie ihre Einkommens- und Vermögensverhältnisse detailliert darlegen sollten, obwohl sie dem Arbeitsamt erklärt hatten, sie hätten genügend Einkommen oder Vermögen und

wollten deshalb gar keine öffentlichen Leistungen, wie z. B. Arbeitslosenhilfe, erhalten. Sie hatten einen Antrag auf Arbeitslosenhilfe nur gestellt, weil dies grundsätzlich erforderlich ist, damit die Zeiten der Arbeitslosigkeit nach § 58 Abs. 1 Satz 1 Nr. 3 SGB VI für Rentenansprüche angerechnet werden können. Anrechnungszeiten sind nach dieser Vorschrift Zeiten, in denen Versicherte wegen Arbeitslosigkeit beim Arbeitsamt als Arbeitsuchende gemeldet waren und öffentliche Leistungen bezogen oder nur deshalb nicht bezogen haben, weil das zu berücksichtigende Einkommen oder Vermögen dies ausschloß, d. h. weil die Versicherten nicht bedürftig waren.

Auf meine Nachfrage hin hat die BA erklärt, in den Fällen, in denen bei der Arbeitslosmeldung eindeutig erkennbar sei, daß wegen des zu berücksichtigenden Einkommens oder Vermögens eine Gewährung von Leistungen durch das Arbeitsamt nicht in Betracht komme, könne auf einen formellen Antrag verzichtet werden. Dies setze jedoch voraus, daß geeignete Nachweise (Lohn- oder Gehaltsbescheinigung, Rentenbescheinigung, Steuerbescheid etc.) vorgelegt werden. Der Antragsteller müsse in diesen Fällen zwar nicht sein gesamtes Einkommen oder Vermögen nachweisen. Er müsse es jedoch bis zur der Höhe belegen, ab der er im Sinne des SGB III nicht mehr als bedürftig gilt. Die BA begründet dies mit der Verbindlichkeit der Entscheidung des Arbeitsamts für die Rentenversicherungsträger.

Die Vorlage von Einkommens- und Vermögensnachweisen halte ich in den vorliegenden Fällen nicht für erforderlich. Der Gesetzgeber wollte mit der Regelung in § 58 Abs. 1 Satz 1 Nr. 3 SGB VI lediglich ausschließen, daß Zeiten der Arbeitslosigkeit angerechnet werden, in denen der Betroffene aus anderen Gründen als ausreichendes Einkommen oder Vermögen keine öffentlichen Leistungen erhalten hat. Dies ist der Fall, wenn der Betroffene solche Leistungen z. B. aus einem von ihm zu vertretenden Grund nicht erhält, etwa weil er nicht bereit war, an zumutbaren Bildungsmaßnahmen teilzunehmen, und deshalb eine Sperrzeit verhängt wurde oder weil sein Anspruch auf Arbeitslosenhilfe wegen der Versäumung von Meldeterminen beim Arbeitsamt ruht (Säumniszeit). Da das Arbeitsamt Kenntnis vom Vorliegen dieser Umstände hat, genügt es m.E., wenn der Betroffene schriftlich erklärt, genügend eigenes Einkommen oder Vermögen zu haben. Das Arbeitsamt kann daraufhin feststellen, ob die übrigen Voraussetzungen für den Erhalt von Leistungen nach dem SGB III vorliegen und – wenn dies zutrifft – dem Rentenversicherungsträger die Anrechnungszeiten mitteilen. Ich habe dies der BA vorgetragen. Es bleibt abzuwarten, ob eine Lösung des Problems gefunden werden kann, die den berechtigten Anliegen von finanziell abgesicherten Bürgern entspricht, die vom Staat kein Geld, aber ihre Rentenansprüche korrekt berechnet wissen wollen.

20.4 Unterschiedliche Aufbewahrungsfristen für ärztliche und psychologische Gutachten

Für die Aufbewahrung von Gutachten und Befundunterlagen im **Ärztlichen** und im **Psychologischen Dienst der Arbeitsämter** hat die BA schon vor langer Zeit detaillierte Vorgaben durch entsprechende Erlasse gemacht. Danach beträgt die Aufbewahrungsfrist für Gutachten und Befundunterlagen im Ärztlichen Dienst zehn Jahre. Vor etwa 15 Jahren wurde die Aufbewahrungsfrist für entsprechende Unterlagen im Psychologischen Dienst von den damals ebenfalls geltenden zehn Jahren auf fünf Jahre herabgesetzt und datenschutzgerecht vorgeschrieben, wo die einzelnen Ausfertigungen der Gutachten und Befundunterlagen nicht nur im Psychologischen Dienst, sondern auch in der Stelle des Arbeitsamtes (Arbeitsvermittlung, Berufsberatung) aufzubewahren sind, die das Gutachten angefordert haben. Diese Regelungen wurden in den letzten Jahren – zum Teil auf meine Anregung hin (vgl. etwa meine Forderungen im 10. TB S. 64 f.) – präzisiert. Hinsichtlich der Regelungen zur Aufbewahrung der Gutachten und Befundunterlagen im Psychologischen Dienst hatte die BA im Jahr 1986 durch den Runderlaß 175/86 u. a. verfügt, daß die Aufbewahrungsfrist von fünf Jahren auch dann gilt, wenn innerhalb der fünf Jahre ein neues Gutachten erstellt wird. Danach sollte jedes Gutachten *„mit Ablauf des 5. Kalenderjahres nach dem Tag der Begutachtung oder Beratung“* ausgesondert und vernichtet werden. Erst mit dem Runderlaß 64/94 vom 27. Juni 1994 wurde bestimmt, daß die Fünfjahresfrist wiederum zu laufen beginnt, wenn der Psychologische Dienst erneut eingeschaltet wurde. Soweit die datenschutzrechtlich unbedenkliche Theorie.

Daß die Praxis dem nicht immer entspricht, zeigte sich, als sich im Berichtszeitraum ein Petent an mich wandte, weil er bei der Einsicht in die **Leistungsakte** des für ihn zuständigen Arbeitsamts im Rahmen eines sozialgerichtlichen Verfahrens ein für ihn ungünstiges psychologisches Gutachten vorfand, das noch aus dem Jahre 1988 stammte. Zu Recht war er der Auffassung, daß dieses Gutachten für aktuelle Maßnahmen keine Entscheidungsgrundlage mehr sein kann und forderte, das Gutachten aus den Unterlagen zu entfernen. In einer ersten Stellungnahme teilte mir die BA mit, daß das Arbeitsamt das psychologische Gutachten aufgrund des oben genannten Runderlasses 175/86 nach Ablauf der fünfjährigen Aufbewahrungsfrist gelöscht habe. Bei einer Kontrolle im Arbeitsamt konnte ich allerdings feststellen, daß die BA nur den Psychologischen Dienst des Arbeitsamts nach dem fraglichen Gutachten gefragt hatte. Dieser hatte wahrheitsgemäß geantwortet, daß er das Gutachten den Vorschriften entsprechend gelöscht hatte. Allerdings hatte der Psychologische Dienst das Gutachten nicht von sich aus, sondern im Auftrag der Abteilung Arbeitsvermittlung und Arbeitsberatung (Abt. AVuAB) des Arbeitsamts erstellt und dorthin ein Exemplar des Gutachtens übermittelt, wo es sich nunmehr noch in der Leistungsakte befand. Bei der Bearbeitung des Sachverhalts stellte ich außerdem fest, daß das Arbeitsamt Mitte der neunziger Jahre eine weitere Akte für Rehabilitationsmaßnahmen **(Reha-Akte)** für den Petenten angelegt hat, die ebenfalls mit einer Kopie dieses psychologischen Gutachtens aus dem Jahr 1988 beginnt.

Bedenken gegen die Übermittlung des Gutachtens an die Abt. AVuAB des Arbeitsamtes bestehen nicht:

Die Übermittlung ist gesetzlich und durch Erlasse der BA geregelt und vor allem für die Aufgabenerfüllung der Abt. AVuAB grundsätzlich erforderlich.

Die Aufbewahrung des Gutachtens aus dem Jahre 1988 in der Leistungsakte der Abt. AVuAB über die erforderliche Dauer hinaus ist jedoch ebenso unzulässig wie die Tatsache, daß die Abt. AVuAB des Arbeitsamts das Gutachten entgegen der Vorschriftenlage nicht in einem gesonderten Ordner abgeheftet, sondern in der Leistungsakte aufbewahrt hat. Die eingangs geschilderten Regelungen über die Aufbewahrung von Gutachten gelten allerdings nur für den Ärztlichen und den Psychologischen Dienst der Arbeitsämter, nicht aber für die Abt. AVuAB und andere Stellen innerhalb des Arbeitsamts. Jedoch regelt ein Runderlaß aus dem Jahr 1989, daß psychologische Gutachten in der Abt. AVuAB sowohl bei laufenden als auch bei erledigten Bewerberangeboten *„in gesonderten Ordnern abzuheften und in verschließbaren Schränken aufzubewahren“* sind.

Hinsichtlich der Dauer der Aufbewahrung des Gutachtens aus dem Jahre 1988 gilt folgendes:

Wenn der Psychologische Dienst bereits das in Frage stehende Gutachten weisungsgemäß nach fünf Jahren vernichtet hat, läßt sich dessen Aufbewahrung in einer anderen Abteilung des Arbeitsamts für einen weitaus längeren Zeitraum nicht rechtfertigen. Dies gilt insbesondere auch für die Aufnahme einer Kopie des Gutachtens in die erst später angelegte Reha-Akte. Die Unverhältnismäßigkeit der langen Aufbewahrungsdauer wird besonders deutlich, wenn man berücksichtigt, daß die BA für die Verwendung von ärztlichen Vorgutachten durch Ärzte bereits vor mehr als 10 Jahren festgelegt hat, nach einem halben Jahr dürften diese grundsätzlich nicht mehr Grundlage für ein Gutachten nach Aktenlage sein (vgl. 10. TB S. 64). Für die Verwendung psychologischer Gutachten jedenfalls für Stellen außerhalb des Psychologischen Dienstes muß dies entsprechend gelten. Ich halte es daher für nicht vertretbar, für die Vermittlungstätigkeit ein inzwischen 10 Jahre altes psychologisches Gutachten aufzubewahren.

Unzulässig war es darüber hinaus, daß eine Kopie des Gutachtens Mitte der neunziger Jahre in die neu angelegte Reha-Akte abgeheftet wurde. Aus welchem Grund die Reha-Akte mit dem Gutachten aus dem Jahr 1988 beginnt, ist nicht nachvollziehbar, da dieses Gutachten mit den beabsichtigten Rehabilitationsmaßnahmen in keinerlei Zusammenhang steht.

Im übrigen kommt hinzu, daß der Petent in den letzten Jahren vom Psychologischen Dienst des Arbeitsamts regelmäßig begutachtet wurde, so daß laufend neue Befunde über ihn vorhanden waren. Warum weiterhin dann das Gutachten aus dem Jahr 1988 herangezogen wurde, ist nicht nachzuvollziehen.

Ich habe die Aufbewahrung des Gutachtens aus dem Jahr 1988 in der Leistungs- und in der Reha-Akte gegenüber der BA wegen Verstoßes gegen die §§ 67b Abs. 1, 67c Abs. 1 und 2 SGB X **beanstandet** und sie aufgefordert, das fragliche Gutachten und dessen Kopien zu vernichten. Eine Stellungnahme der BA hierzu liegt noch nicht vor.

20.5 Unzulässige Weitergabe von Daten über persönliche Verhältnisse

Ein Arbeitsamt ließ im Umgang mit Sozialdaten einer jungen Frau die gebotene Aufmerksamkeit und Umsicht vermissen.

Die junge Frau, die sich an mich wandte, ist Kind aus der ersten Ehe ihrer Mutter. Bereits seit ihrem zweiten Lebensjahr lebt sie mit ihrer Mutter und ihrem Pflegevater zusammen, dessen Namen sie auch angenommen hat. Mit ihrem leiblichen Vater hatte die Petentin keinen Kontakt.

Der leibliche Vater der Petentin hatte einen Antrag auf Arbeitslosengeld gestellt. Das Arbeitsamt benötigte nähere Angaben für dessen Berechnung, da sich in den Antragsunterlagen ein Hinweis auf die Petentin als Tochter des Antragstellers befand. Nach § 129 SGB III erhält ein Arbeitsloser einen erhöhten Leistungsansatz an Arbeitslosengeld, wenn er mindestens ein Kind hat. Ist dieses – wie im vorliegenden Fall – bereits volljährig, dürfen dessen Einkünfte allerdings gewisse Höchstgrenzen nicht überschreiten. Um diese Frage zu klären, wandte sich das Arbeitsamt unmittelbar an den Ausbildungsbetrieb der Petentin, wobei es mitteilte, daß der Antragsteller auf Arbeitslosengeld der leibliche Vater der Petentin ist.

Das Arbeitsamt hat mit seiner Mitteilung gegenüber dem Ausbildungsbetrieb besonders schützenswerte Daten über die Familienverhältnisse der Petentin offenbart. Es hat nicht nur bekanntgemacht, wer der leibliche Vater der Petentin ist, sondern damit zugleich auch preisgegeben, daß ihr Pflegevater, dessen Namen sie trägt, nicht ihr leiblicher Vater ist.

Die Anfrage beim Arbeitgeber der Petentin einschließlich der Unterrichtung darüber, wer ihr leiblicher Vater ist, war unzulässig. Eine gesetzliche Grundlage hierfür gibt es nicht. Die in Frage stehenden Daten hätten beim Vater selbst erhoben werden müssen.

Von einer Beanstandung nach § 25 BDSG dieses erheblichen Verstoßes gegen das Sozialgeheimnis habe ich nur abgesehen, weil ich darin ein Fehlverhalten einzelner Mitarbeiter des Arbeitsamtes in einem besonders gelagerten Fall sehe. Sowohl die BA als auch das zuständige Landesarbeitsamt haben das unzulässige Vorgehen des Arbeitsamtes und die daraus entstandenen Folgen für die Petentin ausdrücklich bedauert. Das Arbeitsamt hat sich bei der Petentin entschuldigt. Mir wurde versichert, daß die zuständigen Mitarbeiter des Arbeitsamtes auf die fehlerhafte Verfahrensweise und die einschlägigen Bestimmungen zum Datenschutz hingewiesen wurden, so daß mit einer Wiederholung nicht zu rechnen ist.

Der Fall macht deutlich, wie wichtig es ist, auch bereits bei Anfragen zur Aufklärung eines Sachverhalts auf die datenschutzrechtlichen Erfordernisse zu achten.

20.6 „Schulter an Schulter“ im Arbeitsamt

Im Rahmen meiner Beratungs- und Kontrolltätigkeit bei den Arbeitsämtern und durch Eingaben betroffener Bürger wurde ich darauf aufmerksam, daß in den für die Ar-

beitsvermittlung und Arbeitsberatung zuständigen Abteilungen in vielen Fällen in den dortigen Anmeldestellen zwei Bedienstete des Amtes in einem Dienstraum zu gleicher Zeit die Anträge von zwei Antragstellern entgegennehmen. Bei der Übertragung der in den Anträgen enthaltenen Angaben in die automatisierte Datenverarbeitung werden diese Daten vor dem eigentlichen Einzel- bzw. Beratungsgespräch auch schon an dieser Stelle erörtert. Dabei sitzen die Antragsteller manchmal sogar nebeneinander, so daß die zum Teil besonders schützenswerten Daten – wie z. B. Informationen über die augenblickliche finanzielle Situation, Scheidungsabsichten oder die Dauer eines Gefängnisaufenthalts – gleichzeitig anwesenden weiteren Antragstellern zwangsläufig zur Kenntnis gelangen.

Bedauerlicherweise hat die BA die von mir festgestellten datenschutzrechtlichen Verstöße gegen das Recht auf informationelle Selbstbestimmung und gegen das Sozialgeheimnis nach § 35 SGB I bislang nicht in allen Fällen abgestellt. Sie begründet dies damit, daß in den betroffenen Arbeitsämtern aus räumlichen und haushaltsbedingten Gründen eine andere Unterbringung der Bediensteten oder das Einziehen von Trennwänden nicht möglich ist.

Ich stehe mit der BA hierzu noch im Gespräch; sollten datenschutzgerechte Lösungen – z. B. durch Änderung des Organisationsablaufs in den jeweiligen Stellen der Arbeitsämter – seitens der BA nicht gefunden werden, werde ich von der von mir bereits angedrohten förmlichen Beanstandung nicht absehen können.

20.7 Übermittlung von Daten Arbeitsuchender an Private

Um möglichst viele Arbeitsuchende wieder in Arbeit zu vermitteln, bedienen sich die Arbeitsämter auch der Hilfe privater Unternehmer. Dies erfordert allerdings, daß die Arbeitsämter diesen personenbezogene Daten von Arbeitsuchenden mitteilen. Der Gesetzgeber hat hierfür vorgesehen, daß personenbezogene Daten an die privaten Stellen nur übermittelt werden dürfen, wenn die vorherige schriftliche Einwilligung des betroffenen Arbeitsuchenden vorliegt (§§ 37 Abs. 2 SGB III, 67b Abs. 2 SGB X). Darüber hinaus hat die BA in mehreren Erlassen besondere Regelungen zur Beteiligung privater Dritter getroffen, in denen u. a. auf die Notwendigkeit der Einholung der schriftlichen Einwilligung der Arbeitsuchenden ausdrücklich hingewiesen wird.

Die Vorschriftenlage für die Arbeitsämter ist somit eindeutig und datenschutzgerecht. Gleichwohl haben sich einige Arbeitsuchende an mich gewandt, weil das örtlich zuständige Arbeitsamt ihre personenbezogenen Daten an einen privaten Arbeitsvermittler oder an einen privaten Anbieter von Schulungsmaßnahmen weitergeleitet hatte, ohne daß ihre schriftliche Einwilligung hierzu eingeholt worden war. Die BA sprach zunächst von Einzelfällen. Allerdings kann man nach der Anzahl der Eingaben und der sicherlich gegebenen Dunkelziffer kaum noch von Einzelfällen sprechen.

Aus Gesprächen anläßlich von Kontrollen bei Arbeitsämtern weiß ich von Klagen der Mitarbeiter über die Vielzahl der Erlasse der BA. Ich bleibe mit der BA darüber im Gespräch, wie zu erreichen ist, daß die Mitarbeiter der Arbeitsämter über wichtige gesetzliche und sonstige Regelungen – insbesondere auch datenschutzrechtlich bedeutsame Regelungen – rechtzeitig und ausreichend unterrichtet sind.

21 Krankenversicherung

21.1 Das Datenschutzkonzept der gesetzlichen Kassen muß besonders die Zweckbindung berücksichtigen

Der Einsatz der Informationstechnik sowie Aufbau und Organisation der Kassen sind gegenwärtig erheblichen Veränderungen unterworfen. Von Bedeutung sind dabei die folgenden Entwicklungen:

- Der elektronische Datenaustausch zwischen Leistungserbringern und den gesetzlichen Kassen führt zu wesentlichen Änderungen bei Art und Umfang der automatisierten Verarbeitung von Versichertendaten. Krankenversicherungsdaten stehen in weit größerem Umfang als bisher in elektronischer Form und damit automatisiert auswertbar zur Verfügung.
- Insbesondere bei Kassen mit Geschäftsstellenstruktur vollziehen sich zum Teil einschneidende Organisationsänderungen. Spezialisierte Aufgabenbereiche werden durch Funktionsbereiche mit vergleichsweise grober Unterteilung nach Aufgabengesichtspunkten abgelöst (z. B. Privatkundenservice). Hintergrund ist die angestrebte umfassende Kundenbetreuung durch Gruppen, innerhalb derer jede Aufgabe grundsätzlich durch alle Mitarbeiter wahrgenommen werden kann („one face to the customer“). Dies führt i.d.R. zu umfangreichen Zugriffsrechten der Mitarbeiter.
- Wesentliche DV-Produktionsarbeiten werden, auch kassenübergreifend, auf zentrale Stellen konzentriert, die auf der Basis des § 80 SGB X (Datenverarbeitung im Auftrag) tätig werden.
- Nach den Reformen im Gesundheitsbereich und der Einführung wettbewerbsähnlicher Strukturen kommen Mitgliederwerbung und -pflege, Aufklärung und Kostenmanagement steigende Bedeutung zu. Dies kann dazu führen, daß Sozialdaten für Zwecke genutzt werden, die durch bestehende rechtliche Verarbeitungsbefugnisse nicht gedeckt sind.
- Wirtschaftlichkeitsprüfungen, Abrechnungsprüfungen und Qualitätssicherungsmaßnahmen beruhen zwar auf unterschiedlichen Rechtsgrundlagen, sind aber der Sache nach eng miteinander verzahnt und gewinnen zunehmend an Bedeutung.

Diese Entwicklungen in der gesetzlichen Kranken-/Pflegeversicherung sind vor dem Hintergrund des Einsatzes moderner Datenbanksysteme zu sehen. Diese sind für die Verwaltung großer Datenmengen konzipiert. Es handelt sich dabei um eine integrierte Sammlung von Daten, die eine für viele Anwendungen nutzbare Datenbasis darstellt. In einem sog. Datenbankmanagementsystem – DBMS – werden die Anwendungsprogramme

von der Datenbasis getrennt verwaltet. Datenbankoperationen können dabei über eine standardisierte freie Abfragesprache (**S**tandard **Q**uery **L**anguage) durchgeführt werden, deren Sprachumfang komplexe logische Operationen und damit umfassende Datenbankauswertungen ermöglicht.

Die Struktur einer relationalen Datenbank steht der Umsetzung der gesetzlich vorgegebenen Zweckbindungsanforderungen im Grundsatz insbesondere durch zwei Aspekte entgegen:

– Relationale Datenbanken sind sehr flexibel organisiert, d. h. Daten sind zunächst unabhängig vom konkreten Verwendungszweck an jeder beliebigen Stelle in einem Netzwerk gespeichert.
– Auf die Daten einer relationalen Datenbank kann bei mangelnder Organisation der Rechte (wer darf was und wie mit welchen Programmen und Daten tun) ohne Restriktionen durch Anwendungsprogramme immer mittels einer freien Abfragesprache zugegriffen werden.

Durch diese skizzierten technischen Rahmenbedingungen besteht die Gefahr, daß Zweckbindungs- und Zugriffsregeln umgangen werden.

Das Sozialgesetzbuch enthält allerdings bereits ein umfangreiches datenschutzrechtliches Regelungswerk, um dieser Gefahr zu begegnen. Der gesetzgeberischen Systematik folgend sind insoweit insbesondere die drei folgenden datenschutzrechtlichen Kategorien maßgebend:

Erhebung und Speicherung für zulässige Zwecke, Zweckbindung und aufgabenorientierte Zugriffsrechte sowie Löschung.

Rechtsgrundlage für die Erhebung und Speicherung von Sozialdaten ist § 284 Abs. 1 Satz 1 SGB V bzw. § 94 Abs. 1 SGB XI.

Die Zulässigkeit einer Zweckänderung beurteilt sich nach § 284 Abs. 3 SGB V bzw. § 94 Abs. 2 SGB XI. Nach diesen Vorschriften i.V.m. § 67c SGB X dürfen die Kranken-/Pflegekassen die von ihnen rechtmäßig gespeicherten Daten auch für andere Zwecke nutzen. Allerdings enthalten § 284 Abs. 1 Sätze 2 bis 4 und Abs. 2 SGB V Zweckbindungsgarantien für versichertenbezogene Daten, die auf Datenbändern oder anderen maschinell verwertbaren Datenträgern gespeichert sind. Desgleichen enthält § 292 Abs. 2 Satz 3 SGB V eine spezielle Zweckbindungsgarantie.

Löschungsvorgaben sind zum Teil in § 304 SGB V sowie § 107 SGB XI enthalten. Für die hiervon nicht erfaßten Sozialdaten sind gem. § 84 Abs. 2 SGB X Löschungsfristen vorzusehen.

Soweit Verfahren zur Befriedigung möglicher individueller Serviceinteressen der Versicherten und über die unabdingbare Aufgabenerfüllung des Leistungsträgers hinausgehend konzipiert werden, muß die datenschutzrechtliche Vorgabe umgesetzt werden, wonach der einzelne grundsätzlich selbst über die Preisgabe und Verwendung seiner personenbezogenen Daten zu bestimmen hat.

Vor diesem rechtlichen und tatsächlichen Hintergrund habe ich einige Lösungsansätze für das Problem entwikkelt, wie die gesetzlich vorgegebene Zweckbindung von den Leistungserbringern eingehalten werden kann, ohne auf neue Informationstechniken zu verzichten. Dabei kann es nach meiner Auffassung nicht ausreichen, eine unzulässige Verarbeitung allein mit technischen Mitteln auszuschließen. Zugleich datenschutzgerechte und praktikable Lösungen bedingen vielmehr, eine den Zweckbindungen zuwiderlaufende Datennutzung möglichst durch das Zusammenwirken technischer Maßnahmen und organisatorischer Verfahrensregelungen zu unterbinden bzw. durch eine transparente Gestaltung der Verfahren erkennbar zu machen. Besondere Bedeutung kommen dabei der Vergabe von Zugriffsrechten gem. § 35 Abs. 1 Satz 2 SGB I, der Protokollierung von Abfragen und Auswertungen sowie der Einhaltung stringenter Löschungsvorgaben zu.

Mit diesen Überlegungen bin ich an die Spitzenverbände der gesetzlichen Kranken- und Pflegekassen sowie an das BMG und das BMA herangetreten. Ich gehe davon aus, daß sie in konkrete Konzepte einfließen werden.

21.2 Datenschutz als Hemmnis für die Aufdeckung betrügerischer Fehlabrechnungen?

Immer wieder wird – gerade auch von Kassenseite – der Vorwurf erhoben, datenschutzrechtliche Vorgaben behinderten die Aufdeckung von Abrechnungsmanipulationen von Leistungserbringern. Bei einer großen Ersatzkasse konnte ich mir hierzu einen Eindruck von der Komplexität des Geschehens verschaffen.

Es hat sich gezeigt, daß im Hinblick auf die unterschiedliche gesetzliche Ausgestaltung jeweils zwischen der Abrechnungs- und Wirtschaftlichkeitsprüfung sowie der Qualitätsprüfung und hierzu korrespondierend zwischen den einzelnen Leistungserbringern (Ärzte, Zahnärzte, Krankenhäuser, Apotheken und sonstige Leistungserbringer) zu differenzieren ist.

Ausgangspunkt der Überlegungen ist die Frage, ob die einzelnen Prüfungen von der abschließenden Aufgabenbeschreibung der Kassen in § 284 SGB V abzuleiten sind. Hierzu vertrete ich die folgende Auffassung:

– **Abrechnungsprüfung**

  Für die Kassen fehlt ein ausdrücklicher Hinweis auf die Aufgabe, die Zulässigkeit und Richtigkeit der Abrechnung zu prüfen, wie sie in § 285 Abs. 1 Nr. 2 SGB V für die Kassenärztlichen Vereinigungen enthalten ist. Die unterschiedliche Wortwahl in § 284 Abs. 1 Nr. 8 SGB V (*„Abrechnung“*) und in § 285 Abs. 1 Nr. 2 SGB V (*„Überprüfung der Zulässigkeit und Richtigkeit der Abrechnung“*) läßt nicht zwingend den Schluß zu, daß *„Abrechnung“* die Überprüfung der Zulässigkeit und Richtigkeit der Abrechnung nicht mit umfassen kann, da § 284 Abs. 1 Nr. 8 SGB V die Abrechnung mit jeder Art von Leistungserbringern betrifft und jedenfalls bei den sonstigen Leistungserbringern und den Krankenkäusern die Überprüfung

der Zulässigkeit und Richtigkeit der Abrechnung selbstverständlicher Bestandteil der Abrechnung mit den Kassen ist.

Diese Interpretation wird auch durch die Begründung zu der jetzigen Vorschrift des § 83 Abs. 2 SGB V (Plausibilitätskontrollen durch Kassenärztliche Vereinigungen) gestützt, in der es heißt: *„Abs. 2 verpflichtet die Partner der Gesamtverträge, die Prüfungen ärztlicher Abrechnung so auszugestalten, daß Abrechnungsmanipulationen verhindert werden. Die Regelung schließt weitere Prüfungen durch die Krankenkassen nicht aus.“* (Drucksache 11/2237 vom 3. Mai 1988, S. 193 – zum damaligen § 91 des Entwurfs).

Die erwähnte Ersatzkasse hat darauf hingewiesen, daß die Abrechnungsprüfung wegen der lediglich fallbezogenen Abrechnung nach § 295 Abs. 2 SGB V wesentlich begrenzt ist. Als ein nachvollziehbares Beispiel wurde darauf hingewiesen, daß ambulante vertragsärztliche Leistungen nach stationären Grundsätzen vergütet werden, wenn der Versicherte an demselben Tag in die stationäre Behandlung des Vertragsarztes (Belegarztes) aufgenommen wird. Durch die ausschließlich fallbezogene Übersendung von Abrechnungsdaten ist eine Prüfung insoweit nicht möglich.

– **Wirtschaftlichkeitsprüfung**

Wirtschaftlichkeitsprüfungen sind als Aufgabenzuweisung für die Kassen ausdrücklich lediglich für Ärzte, Zahnärzte und für im Krankenhaus ambulant erbrachte Leistungen gem. § 284 Abs. 1 Nr. 9 i.V.m. § 106 SGB V vorgesehen.

Allerdings finden sich Aussagen zur Wirtschaflichkeit der Leistungserbringung in § 113 SGB V für die Krankenhausbehandlung, in § 125 SGB V für die Versorgung mit Heilmitteln und in §§ 126, 127 SGB V für die Leistungserbringung mit Hilfsmitteln. Auch die Vorgaben des § 129 SGB V zur Ausgestaltung der Rahmenverträge über die Arzneimittelversorgung beschreiben Aspekte der Wirtschaftlichkeit.

In diesem Bereich bedarf es wegen der unterschiedlichen Vorgaben einer besonderen Diskussion, ob und in welchem Umfang Kassen eventuell nach § 284 Abs. 1 Nr. 4 i.V.m. §§ 2 und 12 SGB V befugt sind, personenbezogene Daten zu erheben und speichern.

– **Qualitätsprüfung**

Keine ausdrückliche Befugnis zur Erhebung und Speicherung personenbezogener Daten für Zwecke der Qualitätsprüfung enthält § 284 SGB V, anders als § 285 Abs. 1 Nr. 6 i.V.m. § 136 SGB V, wo dies klar geregelt ist. Allerdings könnte eine entsprechende Befugnis gem. § 284 Abs. 1 Nr. 4 i.V.m. § 2 Abs. 1 Satz 3 SGB V angenommen werden. Eine Bestätigung hierfür findet sich in § 298 SGB V, wonach im Rahmen eines Prüfverfahrens versichertenbezogene Angaben an die Kassen übermittelt werden dürfen, die die Qualität der ärztlichen Behandlungs- oder Verordnungsweise im Einzelfall betreffen. Es kann nicht davon ausgegangen werden, daß der Gesetzgeber eine Übermittlungsbefugnis auf Leistungserbringerseite ohne eine entsprechende Erhebungs- und Speicherungsbefugnis auf Kassenseite hat festlegen wollen. Die Befugnis der Kassen darüberhinaus Qualitätsprüfungen durchführen, müßte daher vom Gesetzgeber – wie in § 285 Abs. 1 Nr. 6 SGB V – konkretisiert werden.

Die Ersatzkasse hat mir gegenüber zu Recht darauf hingewiesen, daß bereits jetzt ein genereller Auftrag für die Kassen nach § 2 Abs. 4 SGB V besteht, auf eine wirksame Gewährung von Leistungen zu achten. Auch hier wird daher die Diskussion an der Frage anzusetzen haben, ob und in welchem Umfang § 284 Abs. 1 Nr. 4 SGB V die personenbezogene Erhebung und Speicherung für Qualitätsprüfungen zuläßt.

Die von mir skizzierten Auffassungen betreffen vor allem das Verhältnis zwischen Leistungserbringer und Kasse. Im Rahmen eines zunehmend diskutierten indikations- bzw. vorgangsbezogen Fallmanagements ergeben sich dann noch folgende Fragen zur datenschutzrechtlichen Position des Versicherten:

- Unter welchen Voraussetzungen dürfen personenbezogene Leistungskonten der Versicherten – etwa durch zweckändernde Zusammenführung von zu verschiedenen Zwecken an die Kassen übermittelten Daten – geführt werden?
- Ist der Versicherte über Prüfverfahren zu informieren, in denen seine personenbezogene Daten Gegenstand einer leistungserbringerbezogenen Auswertung sind und falls ja, in welchem Umfang?

Insgesamt kann ich dem pauschalen Vorwurf, datenschutzrechtliche Regelungen behinderten die Aufdekkung von Abrechnungsmanipulationen, nicht folgen. Das zeigen auch meine vorstehenden rechtlichen Überlegungen. Das Problem scheint mir vielmehr zu sein, daß datenschutzrechtliche Vorgaben der unabweislichen Aufgabenerfüllung der Kassen in Abwägung zu den Grundrechtspositionen der Versicherten und Leistungserbringer nicht konsequent durchformuliert wurden.

Wegen der vielfältigen grundsätzlichen Aspekte habe ich bereits das BMG und die Spitzenverbände der gesetzlichen Krankenversicherung um eine Stellungnahme zu meinen Auffassungen und den noch offenen Fragen gebeten.

21.3 Auskunfspflichten der Leistungserbringer gegenüber Versicherten

Am 1. Juli 1997 ist § 305 Abs. 2 SGB V in Kraft getreten, wonach die Versicherten über die von ihnen in Anspruch genommenen ärztlichen, zahnärztlichen und Krankenhausleistungen sowie die damit verbundenen Ausgaben der Krankenkassen innerhalb von vier Wochen nach Ablauf des Quartals, in dem die Leistungen in Anspruch genommen wurden, zu unterrichten sind. Einzelheiten des Verfahrens sollen von den Spitzenverbänden der Krankenkassen, der Kassenärztlichen und Kassenzahnärztlichen Bundesvereinigung sowie der Deutschen Krankenhausgesellschaft durch Verträge geregelt werden.

Zu meinem Bedauern sind diese Verträge bis heute nicht abgeschlossen. Von Seiten der Kassenärztlichen Bundesvereinigung wird argumentiert, daß eine Unterrichtung des Versicherten über die von den Krankenkassen zu zahlenden Entgelte erst dann möglich sei, wenn für die ärztlichen Leistungen feste Punktwerte vereinbart sind. Die Kassen hingegen verweisen darauf, daß eine Unterrichtung über die Kosten ärztlicher Leistungen auch an Hand des letzten bekannten Abrechnungswertes realisierbar sei.

Auch ich sehe die Schwierigkeiten einer fristgerechten Information im Rahmen budgetierter Versorgungsformen. Der Unterrichtungspflicht der Leistungserbringer kommt jedoch aus meiner Sicht eine besondere Bedeutung zu, da sie wesentlich dazu beiträgt, daß die gespeicherten und übermittelten Behandlungs- und Abrechnungsdaten für den Patienten transparent sind. Daher halte ich die Information des Patienten über den letzten bekannten Abrechnungswert, der ihm zumindest einen Überblick über die Größenordnung der Ausgaben in Relation zu den erbrachten Leistungen verschafft, für einen richtigen und weiter zu verfolgenden Ansatz.

21.4 Umsetzung datenschutzrechtlicher Vorgaben stößt bei der Neustrukturierung der Bahnbetriebskrankenkasse auf große Probleme

Über die Bemühungen der Bahnbetriebskrankenkasse und den Umfang der erforderlichen Umsetzung der gesetzlichen Vorgaben zum Datenschutz habe ich in meinem 16. TB im Zusammenhang mit der Kontrolle der früheren Reichsbahnbetriebskrankenkasse ausführlich berichtet (vgl. 16. TB Nr. 21.5). Eine Nachkontrolle hat im wesentlichen folgendes ergeben:

– **Zur automatisierten Datenverarbeitung:**

Im Bereich der automatisierten Datenverarbeitung, die ich bei einer Geschäftsstelle der Bahnbetriebskrankenkasse kontrolliert habe, konnte ich zahlreiche Verbesserungen vorschlagen. Im Vordergrund standen hierbei die Sicherheit der eingesetzten PC, die Benutzerverwaltung, Regelungen zur Wartung der Server und der PC, die Entsorgung der Datenträger sowie die Sicherheit tragbarer Rechner.

– **Zum internen Datenschutzbeauftragten:**

Erfreulicherweise hat sich der Stellenwert des internen Datenschutzbeauftragten dahingehend geändert, daß er auf dem Gebiet des Datenschutzes unmittelbar dem Vorstand der Bahnbetriebskrankenkasse unterstellt ist. Der ihm zur Verfügung stehende Zeitanteil entspricht m.E. allerdings nicht dem Arbeitsanfall im Bereich Datenschutz. Mit Blick auf die Anzahl der Versicherten nach der Vereinigung der Bundesbahn-Betriebskrankenkasse und der Reichsbahn-Betriebskrankenkasse zur Bahn-Betriebskrankenkasse und die deswegen erforderliche Umsetzung datenschutzrechtlicher Vorgaben in Dienstanweisungen und in dem immer noch nicht überarbeiteten Organisations- und Prozeßhandbuch ist es dringend geboten, die Arbeitskapazität des Datenschutzbeauftragten für die Aufgaben nach § 81 SGB X i.V.m. § 37 Abs. 1 BDSG freizuhalten und ihm gegebenenfalls personelle Unterstützung zu gewähren. Auch die in die gleiche Richtung gehende Forderung des Bundesversicherungsamtes aus dem Jahre 1994 war zum Zeitpunkt meiner Nachkontrolle nicht umgesetzt. Eine entsprechende Stellungnahme der Bahnbetriebskrankenkasse zu diesem Punkt steht noch aus.

– **Zur Organisation des Schutzes der Sozialdaten:**

Während der Nachkontrolle wurde mir seitens der Kasse zum wiederholten Male zugesichert, mir eine zentrale Dienstanweisung zur Organisation des Datenschutzes bei der Postverteilung und dem Botendienst vorzulegen. Bereits im Anschluß an meine Kontrolle im Jahre 1995 hatte ich der Kasse mitgeteilt, daß ich mir hinsichtlich dieses Punktes eine förmliche Beanstandung vorbehalte. Dennoch wurde trotz mehrerer, auch telefonischer Nachfragen meiner Forderung nach organisatorischen Vorgaben zum Schutz der Sozialdaten vor unbefugter Einsicht in diesen Bereichen der Bahnbetriebskrankenkasse bis heute nicht Rechnung getragen. Diese Verfahrensweise habe ich gemäß § 81 Abs. 2 SGB X i.V.m. § 25 BDSG als Verstoß gegen § 78a SGB X und wegen mangelnder Unterstützung bei der Erfüllung meiner Aufgaben als einen Verstoß gegen § 24 Abs. 1 BDSG **beanstandet**. Gleichzeitig habe ich die Bahn-BKK gebeten, mir die ausstehende zentrale Dienstanweisung nunmehr unverzüglich zu übersenden.

21.5 Zeitpunkt für die Einführung eines Schlüssels nach ICD–10 noch offen

Mit der Automatisierung der Datenübermittlung zu Abrechnungszwecken verpflichtete der Gesetzgeber Ärzte und Krankenhäuser zur Codierung der zu übermittelnden leistungsbegründenden Diagnosen nach dem ICD-10-Schlüssel als Ersatz zum bisher üblichen Klarschrifteintrag. Nachdem dieser angeordnete Schlüssel, den die Weltgesundheitsorganisation für globale Statistik- und Forschungszwecke entwickelt hatte, auf heftige Kritik u. a. im Hinblick auf die Eignung zur Begründung der Abrechnung gestoßen war, wurde er von einem Arbeitsausschuß überarbeitet (vgl. 16. TB Nr. 21.1.5).

In meiner Stellungnahme zu der vorgelegten Fassung des Arbeitsausschusses (Version 1.0; Stand: 12. Sept. 1997) habe ich insbesondere auf zwei Gesichtspunkte hingewiesen:

– Nach dem Gesetzeswortlaut des § 295 Abs. 1 Satz 2 SGB V sind „Diagnosen“ zu verschlüsseln. Zumindest bei den folgenden Verschlüsselungen ist es fraglich, ob es sich um Diagnosen handelt:

  In dem Kapitel XX sind Fälle zusammengefaßt, die zum einen sinnvolle Krankheitsursachenbeschreibungen darstellen können (z. B. W87.9: Verbrennung durch elektrischen Strom), zum anderen aber einen Hinweis auf die Leistungspflicht bzw. Regreßmög-

lichkeiten darstellen (z. B. X84.9: Vorsätzliche Selbstschädigung).

Auch wenn dringende Bedürfnisse der Praxis angegeben werden, Verschlüsselungen, wie beispielsweise R46.0 (Stark vernachlässigte Körperpflege), für Abrechnungszwecke zu verwenden, kommt die Zulässigkeit derartiger Verschlüsselungen nur in Ausnahmefällen im Zusammenhang mit einer Diagnose in Betracht und ohne Diagnose nur dann, wenn eine solche nicht gestellt werden konnte und gleichwohl eine damit zu begründende Leistung abzurechnen ist.

Schließlich ist vor dem Hintergrund, daß die Vorschrift des § 295 Abs. 1 Nr. 2 SGB V zwischen Diagnose und Befund trennt, die Zulässigkeit der Verschlüsselungen R70 bis R79 (Abnorme Blutuntersuchungen ohne Vorliegen einer Diagnose) sehr fraglich.

– Die Regelung des § 295 Abs. 1 Satz 2 SGB V sieht zudem die Verwendung eines vierstelligen Schlüssels vor. Bei der beabsichtigten Verwendung der Zusatzkennzeichen „V“ (Verdacht auf), „Z“ (Zustand nach), „A“ (Ausschluß von), „R“ (rechts), „L“ (links) und „B“ (beiderseitig) wird der vorgeschriebene vierstellige Schlüssel entgegen dem Gesetzeswortlaut nicht eingehalten.

  In den 1997 zur Praktikabilität und Funktionalität der Verschlüsselung mit dem ICD-10 durchgeführten Modellversuchen in Niedersachsen und Sachsen-Anhalt sind von einem Teil der niedergelassenen Ärzte weitere Zusatzkennzeichen befürwortet worden, wie z. B. Unterscheidungen nach dem Schweregrad in „l“ (leicht), „m“ (mittel) und „s“ (schwer).

In den angeführten Fällen bedarf es einer Prüfung, ob die Angaben erforderlich sind, um eine sachgerechte Abrechnung ärztlicher Leistungen zu gewährleisten, und wenn auf der Basis der ICD-10-Schlüssel ein geeigneter Katalog von Angaben erarbeitet ist, die bei der Abrechnung ärztlicher Leistungen als Begründung dienen können, so verlangt dessen Anwendung für diesen Zweck eine entsprechende Anpassung von § 295 Abs. 1 Satz 2 SGB V. Das BMG hat mir hierzu mitgeteilt, daß zur Zeit nicht absehbar sei, wann eine überarbeitete Fassung des Schlüssels in Kraft gesetzt wird und ob es § 295 SGB V ändern will. Bis dahin schreiben die Ärzte weiter Klartext.

22 Rentenversicherung

22.1 Online-Verfahren zur Verbesserung der Servicefreundlichkeit in der gesetzlichen Rentenversicherung

In den letzten Jahren hat sich das Selbstverständnis der Sozialversicherungsträger hin zu bürgeroffenen Dienstleistern gewandelt. Servicefreundlichkeit für die Kunden ist ein allgemein anerkanntes Ziel geworden. So hat die gesetzliche Rentenversicherung den Versicherten den Zugang zu fachlicher Beratung im persönlichen Gespräch wesentlich erleichtert. Die nachfolgend beschriebenen Verfahren, die versichertennahen Beratern einen Online-Zugriff auf Rentenversicherten-Konten geben, sind Ausdruck dieser veränderten Kundenorientierung.

22.1.1 Dialogverfahren „Gegenseitige Beauftragung der Rentenversicherungsträger mit der Versicherungsbetreuung“

Dieses Dialogverfahren ermöglicht auf der Grundlage von Vereinbarungen zwischen den 27 Trägern der gesetzlichen Rentenversicherung, daß Rentenversicherte bei jeder angeschlossenen Auskunfts- und Beratungsstelle eines beliebigen Rentenversicherungsträgers Auskunft aus ihrem Rentenversicherungskonto und fachliche Beratung erhalten können. Der aktuelle Stand des Rentenversicherungskontos kann ohne weiteres online abgerufen werden. Beteiligt sind die rund 350 Auskunfts- und Beratungsstellen der Rentenversicherungsträger.

In meinem 16. TB (Nr. 22.3) habe ich über dieses Verfahren und über besondere zu seiner datenschutzrechtlichen Sicherung gebotene Maßnahmen berichtet. Zu den von mir geforderten Maßnahmen zählt, daß sich der Versicherte vor einer Auskunftserteilung durch einen Lichtbildausweis (z. B. Personalausweis) ausweisen muß. Der Verband Deutscher Rentenversicherungsträger hat dieser Forderung nur im Grundsatz zugestimmt. Er möchte den Sachbearbeitern in den Auskunfts- und Beratungsstellen erlauben, in Ausnahmefällen auch Auskünfte an Personen zu erteilen, die sich nicht ausweisen können, wenn sie auf andere Weise von der Identität des Versicherten überzeugt sind, etwa anhand von Fragen, die nur der Versicherte selbst beantworten kann.

Dieser Auffassung kann ich nicht folgen, da sie zu einer Sicherheitslücke führt. Sachbearbeiter und die um Auskunft ersuchende Person kennen sich in der Regel nicht. Das Dialogverfahren soll ja gerade ermöglichen, daß der Versicherte in einer an sich unzuständigen Stelle Auskünfte erhält. Gezielte Fragen, die nur der Versicherte selbst richtig beantworten kann, kann der Sachbearbeiter daher erst stellen und deren Antworten auf Richtigkeit bewerten, nachdem er online auf das Rentenkonto zugegriffen hat. Hier könnte es zu einer unzulässigen Datenübermittlung und Einsichtnahme in das Konto kommen.

Die in der Rentenauskunft enthaltenen Angaben ermöglichen dem Sachbearbeiter keine Fragen zur hinreichenden Eingrenzung der Identität eines sich nicht ausweisenden Versicherten. Enthalten sind einmal Angaben wie Anschrift, ggf. Geburtsname, Geburtsdatum und Angaben über die Stationen des beruflichen Werdegangs, die jeder Interessierte im Umfeld eines Versicherten herausfinden kann. Präzise Angaben (z. B. Datum von Beginn und Ende einer zurückliegenden Beschäftigung) wird der Sachbearbeiter gar nicht erwarten können, denn es ist normal, daß auch der tatsächliche Versicherte dies nicht taggenau in Erinnerung hat. Diese Lücke im Rentenauskunftsverfahren könnte gezielt ausgenutzt werden, Zugang zu einer Rentenauskunft oder einer Auskunft zum Versicherungsverlauf zu bekommen.

Ich habe das BMA und das Bundesversicherungsamt um Stellungnahme gebeten.

22.1.2 Bildschirmunterstützte Aufnahme von Anträgen auf Rentenversicherungsleistungen durch die Versicherungsämter und Gemeinden

Die Erteilung von Auskünften und die Antragsaufnahme in allen Angelegenheiten der Sozialversicherung gehört zu den gesetzlichen Aufgaben auch der Versicherungsämter (§ 92, § 93 SGB IV). Soweit hierfür Angaben aus den Rentenversicherungskonten benötigt werden, fordern die Versicherungsämter diese schriftlich beim zuständigen Rentenversicherungsträger an. Die Versicherten müssen nach Eingang der Auskunft erneut zum Versicherungsamt kommen.

Um das Verfahren bei der Aufnahme von Anträgen auf Versicherungsleistungen (z. B. Rente, Rehabilitation) zu erleichtern und dem Versicherten mehrfaches Vorsprechen zu ersparen, sind die Rentenversicherungsträger daran interessiert, den Versicherungsämtern einen Online-Zugriff auf die Rentenversicherungskonten zu eröffnen. Das BMA hat mich zu dem entsprechenden Vorstoß des Verbandes Deutscher Rentenversicherungsträger um Stellungnahme gebeten.

Der beabsichtigte Online-Zugriff beträfe rund 15 000 Stellen, die nicht Teil der gesetzlichen Rentenversicherung sind und nicht dem Sozialgeheimnis unterfallen. Der Online-Zugriff für die Versicherungsämter kann nur durch eine Rechtsnorm ermöglicht werden.

Gemeinsam mit dem Verband Deutscher Rentenversicherungsträger und dem Arbeitskreis „Gesundheit und Soziales“ der Konferenz der Datenschutzbeauftragten des Bundes und der Länder halte ich folgende Anforderungen für erforderlich, um das gewünschte Online-Verfahren einrichten zu dürfen.

– Die Abrufe sind bei den Rentenversicherungsträgern lückenlos fortlaufend zu protokollieren. Zu jedem Abruf, der nicht innerhalb eines festzulegenden Zeitraumes (z. B. drei Monate) in ein Rentenantragsverfahren mündet, ist seine Berechtigung zu überprüfen. Bei den Rentenversicherungsträgern sind die dafür erforderlichen personellen Kapazitäten vorzusehen und die notwendigen Befugnisse gegenüber den Versicherungsämtern gesetzlich einzuräumen.
– Die Versicherungsämter sind in den Katalog der dem Sozialgeheimnis verpflichteten Stellen in § 35 SGB I aufzunehmen.
– Ein Versicherungsamt darf nur auf Versichertenkonten von Versicherten zugreifen, die im Zuständigkeitsbereich des Versicherungsamtes gemeldet sind.
– Der Online-Zugriff ist auf die in der Praxis tatsächlich benötigten Datenfelder des Rentenversicherungskontos zu beschränken (vgl. § 79 Abs. 2 Satz 2 Nr. 3 SGB X).
– Auf Verlangen des Versicherten ist im Rentenversicherungskonto ein Kennzeichen zu setzen, das sein Konto vom Online-Zugriff ausschließt.
– Tatsache, Zeitpunkt und Inhalt jedes erfolgten Abrufs sind im Rentenversicherungskonto oder der Akte des Versicherten so zu dokumentieren, daß der Versicherte über die Online-Abrufe eine Auskunft erhalten kann.
– Der Online-Zugriff kann nur durch den Versicherten selbst (persönlich) nach Identifizierung durch Lichtbildausweis und schriftlicher Antragstellung veranlaßt werden.
– Bei der technischen Realisierung ist ein hinreichender Standard technischer und organisatorischer Maßnahmen zu gewährleisten.

Dem BMA habe ich vorstehende Voraussetzungen für einen Online-Abruf durch die Versicherungsämter mitgeteilt und auch darauf hingewiesen, daß ich es für notwendig halte, einen Großteil dieser Anforderungen im Gesetz selbst zu regeln. Selbstverständlich kann zur Entlastung des Gesetzes ein Teil auch in einer Rechtsverordnung bestimmt werden (z. B. die eindeutige Identifikation des Auskunftsberechtigten oder besondere Auflagen zur Datensicherheit). Die Pflicht zur lückenlosen Protokollierung aller Abrufe durch Versicherungsämter gehört wegen ihrer besonderen Bedeutung für das Verfahren jedoch ins Gesetz.

Bei Redaktionsschluß lag mir noch keine Stellungnahme des BMA vor, ob das Verfahren überhaupt weiterverfolgt wird.

22.2 Online-Abrufe der Hauptzollämter aus Dateien der Datenstelle der Rentenversicherungsträger

Zur Bekämpfung von Schwarzarbeit, illegaler Beschäftigung und Lohndumping führen Prüfgruppen der Bundesanstalt für Arbeit und der Hauptzollämter örtliche Kontrollen durch. In den Branchen, die für die genannten Verstöße erfahrungsgemäß besonders anfällig sind, wie beispielsweise das Baugewerbe, Gaststätten, Schausteller, Beförderung oder Gebäudereinigung, müssen die Arbeitnehmer ihren Sozialversicherungsausweis bei Kontrollen den Prüfgruppen vorweisen. Gleichwohl entstehen Kontrollücken, z. B. wenn die Arbeitnehmer den Ausweis vergessen haben oder wenn der Ausweis bei Arbeitsaufnahme noch nicht ausgestellt ist. Die örtlichen Kontrollen werden ergänzt durch Auskünfte aus zentralen Dateien der Datenstelle der Rentenversicherungsträger. Diese waren bisher schriftlich eingeholt worden. Um diese Auskünfte aus der Arbeitgeberdatei und der Datei der geringfügig Beschäftigten zu vereinfachen und zu beschleunigen, hatte das BMF für die Hauptzollämter mit dem Verband Deutscher Rentenversicherungsträger (VDR) ein Online-Abrufverfahren vorbereitet. Etwa 150 abfragende Stellen sind vorgesehen. Vor Genehmigung der Verwaltungsvereinbarung hatte mich das BMA um Stellungnahme gebeten.

Das geplante Abrufverfahren ist nach § 79 SGB X vertretbar, wenn Häufigkeit oder Eilbedürftigkeit die Online-Anbindung fordern. Das ist hier der Fall. In meiner Stellungnahme habe ich vor allem darauf gedrungen, Abrufe beiderseitig zu protokollieren und Verfahren sowie Mindestumfang einer regelmäßigen internen Prüfung festzulegen. Immerhin können über die Online-Verbindung zur Datenstelle der Rentenversicherungsträger zu allen Arbeitgebern deren Mitarbeiter und zu allen gemeldeten Arbeitnehmern deren Arbeitgeber abgefragt

werden. Das BMA hat in seine Genehmigung der Verwaltungsvereinbarung entsprechende Auflagen aufgenommen. So hat das BMF das Verfahren für datenschutzrechtliche Prüfungen durch die Hauptzollämter in Abstimmung mit mir festzulegen.

Zum Jahreswechsel 1997/98 zeigte mir das BMF die Inbetriebnahme des Lesezugriffs für eine Reihe von Hauptzollämtern an, obwohl es das Prüfverfahren noch nicht abgestimmt hatte. Weil die Protokolldaten, die Gegenstand der Prüfung sind, jeweils nach sechs Monaten zu löschen sind, wurde der Handlungsbedarf immer dringlicher. Da das BMF dennoch weiterhin keinen Entwurf eines Prüfverfahrens zur Abstimmung vorlegte, habe ich den VDR unterrichtet und dem BMF die örtliche Kontrolle des Abrufverfahrens beim Rechenzentrum der Bundesfinanzverwaltung bei der Oberfinanzdirektion Stuttgart und im Hauptzollamt Singen angekündigt. Der VDR trat seinerseits an das BMF heran mit der Bitte, die Durchführung des automatisierten Abrufverfahrens nicht zu gefährden. Ende Mai 1998 habe ich das BMF nochmals eindringlich auf den im Blick auf das fehlende Prüfverfahren datenschutzwidrigen Zustand hingewiesen.

Bei meiner Kontrolle bezog sich das Rechenzentrum Stuttgart auf sein Schreiben an die Vorsteher der Hauptzollämter, in dem zum Prüfverfahren aber im wesentlichen nur ausgeführt ist, daß der behördliche Datenschutzbeauftragte bei den Hauptzollämtern die sachliche Berechtigung des Abrufs unter Verwendung der Abruf-Protokolle und anhand der Verwaltungsvorgänge prüft. Im Hauptzollamt Singen zeigte sich, daß der dortige Datenschutzbeauftragte kurz zuvor erstmals Protokolldaten des VDR vom Rechenzentrum Stuttgart erhalten hatte. Es stellte sich heraus, daß die Aufzeichnungen auf Seiten des Hauptzollamtes ungeeignet waren, eine Verbindung von einem einzelnen protokollierten Abruf zu dem zugrundeliegenden Verwaltungsvorgang herzustellen. Als Ergebnis meiner Kontrolle muß ich leider feststellen, daß es praktisch nicht möglich war zu prüfen, ob die Abrufe berechtigt waren. Letztlich trägt hierfür das BMF die Verantwortung entsprechend seiner Verpflichtung in der Vereinbarung mit dem VDR, auf die der Genehmigungsbescheid Bezug nahm, ein hinsichtlich seiner Praktikabilität bis zur Arbeitsebene durchdachtes und handhabbares Protokollverfahren festzulegen und in einer Arbeitsanweisung konkret zu beschreiben.

Erschwerend kam hinzu, daß die Protokollroutine des VDR einen Programmfehler enthielt, der dazu führte, daß Abrufe im Protokoll mehrfach ausgewiesen wurden, und als Zeitpunkt des Abrufs einheitlich der Beginn der Online-Sitzung angegeben war.

Im Rahmen einer Besprechung der Fachleute aller beteiligten Stellen (VDR, BMF, Rechenzentrum Stuttgart und aus meinem Haus) wurden dann endlich konkrete Anforderungen aufgestellt, um das Abrufverfahren mit Hilfe der Protokollierungen auf beiden Seiten kontrollieren zu können.

Bei Redaktionsschluß standen die Stellungnahme des BMF zu den vorgeschlagenen Anforderungen und die Abstimmung des Prüfverfahrens mit mir noch aus.

22.3 Datenerhebung durch Zusatzversorgungskassen

Das Zusatzversorgungswerk für Arbeitnehmer in der Land- und Forstwirtschaft e.V. (ZLF) ist eine gemeinsame Einrichtung der Tarifvertragsparteien und gewährt an ehemalige Arbeitnehmer, deren Witwen, Witwer und Vollwaisen eine Ergänzung der gesetzlichen Rente. Finanziert wird das ZLF durch einen monatlichen Beitrag der Arbeitgeber in Höhe von gegenwärtiG 10 DM je ständig beschäftigtem Arbeitnehmer.

Nach dem Tarifvertrag sind die Arbeitgeber verpflichtet, jeden beitragspflichtigen Arbeitnehmer anzumelden. Die Leistungspflicht des ZLF gegenüber einem Arbeitsnehmer bleibt aber auch bestehen, wenn ein Arbeitgeber seiner Beitragsverpflichtung nicht nachkommt. Hinweisen auf tarifvertragsgebundene Arbeitgeber, die möglicherweise ihre Arbeitnehmer nicht angemeldet haben, geht das ZLF daher nach. Verbleiben nach einer Anfrage beim Arbeitgeber Zweifel, so wendet sich das ZLF an die Einzugsstelle für den Gesamtsozialversicherungsbeitrag mit der Bitte um Auskunft über die dort angemeldeten Arbeitnehmer. Die aufgrund der gesetzlichen Meldepflicht (§ 28a SGB IV) bei dieser Einzugsstelle vorliegenden Angaben sind angesichts der regelmäßigen Prüfungen bei den Arbeitgebern (§ 28p SGB VI) und Einzugsstellen (§ 28q SGB IV) zuverlässiger, wohl auch deswegen, weil die Nichtbeachtung der Meldepflichten bußgeldbewehrt ist.

Die Auskünfte der Einzugsstellen sind Übermittlungen von Sozialdaten. Soweit die Auskunftsersuchen auf Zweifelsfälle und die für die Feststellung der Beitragspflicht erforderlichen Angaben beschränkt bleiben, ist § 69 Abs. 1 Nr. 1 3. Variante i.V.m. Abs. 2 Nr. 2 SGB X Rechtsgrundlage für die Übermittlung. Hierbei ist allerdings zu beachten, daß die Übermittlung auf die Sozialdaten beschränkt bleibt, die für die Zwecke der Zusatzversorgungskasse tatsächlich erforderlich sind.

Aufgrund meiner Beratung hat das ZLF sein Erhebungsformular inzwischen reduziert. Zudem habe ich darauf hingewiesen, daß Auskünfte bei Dritten vermieden werden könnten, wenn die Tarifvertragsparteien die vertragliche Auskunftspflicht der Arbeitgeber gegenüber dem ZLF konkretisierten, indem sie beispielsweise vertraglich vereinbaren, durch welche Bescheinigung oder welche auszugsweise Kopie der Arbeitgeber die Zahl seiner Mitarbeiter belegen kann. Das ZLF ist bereit, diesem Vorschlag im Rahmen von Tarifverhandlungen nachzugehen.

22.4 Ausschlußtatbestand Kriegsopferversorgung: Kooperation des Bundesarbeitsministeriums mit dem Simon-Wiesenthal-Center

Anfang 1998 berichteten Zeitungen, das BMA beabsichtige, Daten von Rentenempfängern an das Simon-Wiesenthal-Center in Jerusalem zu geben. In Teilen der Öffentlichkeit wurde dies dahingehend verstanden, daß die Daten aller Bezieher einer Rente aus der gesetzlichen Rentenversicherung oder nach dem Bundesversorgungs-

gesetz übermittelt werden sollten. Viele Bürger haben sich daraufhin besorgt an mich gewandt.

Hintergrund der Meldungen war eine Kooperationsvereinbarung zwischen dem BMA und dem Simon-Wiesenthal-Center. Diese Vereinbarung sieht vor, daß das Simon-Wiesenthal-Center die ihm weltweit vorliegenden oder zugänglichen Daten über Kriegsverbrecher EDV-gerecht aufbereitet und dem BMA zur Verfügung stellt. Das BMA wiederum stellt die Daten den deutschen Versorgungsämtern zur Verfügung, die ihre Daten mit den Kriegsverbrecherdaten abgleichen sollen, um bisher unerkannten Kriegsverbrechern die Kriegsopferrente aberkennen zu können.

In der Vereinbarung hat sich das Simon-Wiesenthal-Center auch bereit erklärt, bei Einzelanfragen in konkreten Verdachtsfällen zu prüfen, ob der ihm zur Verfügung stehende Datenbestand entsprechende Erkenntnisse zuläßt. Dieser Weg kommt aber erst ausnahmsweise, nach ergebnisloser Nutzung aller inländischen Erkenntnisquellen, in Betracht und auch danach erst dann, wenn ein konkreter Verdacht eines Kriegsverbrechens vorliegt. Das BMA hat mir versichert, daß solche Einzelanfragen noch nicht vorgekommen sind.

Überhaupt nicht betroffen von der Vereinbarung sind die Sozialdaten der gesetzlich Rentenversicherten.

Es kann erfreulicherweise festgestellt werden, daß die Pressemeldungen falsch waren. Es ist bedauerlich, daß die Öffentlichkeit verunsichert wurde.

22.5 Beratungsgespräch in der BfA

Mit Vertretern der Bundesversicherungsanstalt für Angestellte (BfA) habe ich im Berichtszeitraum wieder ein Beratungs- und Informationsgespräch zu aktuellen Fragen des Datenschutzes geführt und hierbei u. a. folgende Themen erörtert:

22.5.1 Kurentlassungsberichte: Verbesserungen zugesagt

Ein Petent hatte sich hinsichtlich des Verfahrens der BfA zum ärztlichen Kurentlassungsbericht an mich gewandt und insbesondere die Zustimmungserklärung zur Übermittlung des Berichts an BfA, Hausarzt oder in Auszügen an die gesetzliche Krankenkasse und die internen Regelungen der Einsichtnahme in den Entlassungsbericht problematisiert. Zu grundsätzlichen datenschutzrechtlichen Anforderungen an den Umgang mit den sog. Kurentlassungsberichten, die nach Abschluß medizinischer Rehabilitationsmaßnahmen (Kuren) durch die Träger der Rentenversicherung oder in deren Auftrag vom behandelnden Arzt der Kureinrichtung gefertigt werden, habe ich mich bereits in meinem 8. TB Nr. 10.6.1 geäußert.

Die BfA hat mir im Gespräch bestätigt, daß vom Versicherten die Abgabe der „Erklärung zum Entlassungsbericht“ erst bei bzw. nach dem Abschlußgespräch mit dem Reha-Arzt erwartet wird. Daß der Formularsatz bereits vorher, nämlich wie vom Petenten bemängelt, zu Beginn der Reha-Maßnahme, ausgehändigt wird, soll dem Versicherten ermöglichen, sich die Erläuterungen in Ruhe durchzulesen. Sollte dem Versicherten in der Reha-Einrichtung bereits vor dem Abschlußgespräch die Erklärung zum Entlassungsbericht abverlangt werden, widerspricht dies den Vorgaben der BfA.

Die BfA hat mir zugesagt, das Verfahren zur Abgabe der Erklärungen zum ärztlichen Entlassungsbericht in den Kurkliniken zu überarbeiten und in Details zu ergänzen. Auch hinsichtlich der Einsichtsrechte des Betroffenen in die Berichte beabsichtigt sie, die Anweisungen an die Kliniken und die Aufklärungsschreiben an die Patienten in enger Abstimmung mit mir zu verbessern.

22.5.2 Übermittlung medizinischer Daten zum Schutze des Betroffenen

Ein Petent stellte mir die Frage, inwieweit die BfA als Sozialversicherungsträger berechtigt ist, ein Betreuungsverfahren für einen Versicherten „einzuleiten“.

Nach § 71 Abs. 3 SGB X ist eine Übermittlung von Sozialdaten zulässig, soweit es nach dem pflichtgemäßen Ermessen eines Leistungsträgers erforderlich ist, dem Vormundschaftsgericht die Bestellung eines Betreuers oder eine andere Maßnahme in Betreuungssachen zu ermöglichen.

Nach Auskunft der BfA wurde die vorliegende Thematik dort erstmals 1992 anläßlich eines Einzelfalls geprüft. Danach wurde in einer Dienstanweisung an die BfA-Ärzte festgelegt, daß die Fachabteilung der BfA zur Ausübung des pflichtgemäßen Ermessens im Einzelfall vor einer solchen Übermittlung immer den beratungsärztlichen Dienst der BfA einschaltet. Damit ist eine datenschutzgerechte Verfahrensweise in diesen Fällen sichergestellt.

22.5.3 Behandlung von Sozialversicherungsausweisen

Versicherte, die für die Durchführung der Versicherung sowie für die Feststellung und Erbringung von Leistungen einschließlich der Rentenauskunft erforderliche Daten mit Eintragungen in dem Ausweis für Arbeit und Sozialversicherung nachweisen können, sind berechtigt, in einer beglaubigten Abschrift des vollständigen Ausweises oder von Auszügen des Ausweises die Daten unkenntlich zu machen, die für den Träger der Rentenversicherung nicht erforderlich sind und diese Abschrift dem Träger der Rentenversicherung nach Nachweis vorzulegen (§ 286e SGB VI).

Veranlaßt durch eine Eingabe habe ich mir in der Besprechung das Verfahren der BfA im Umgang mit eingereichten Ausweisen für Arbeit und Sozialversicherung (SV-Ausweis) darstellen lassen. Danach sind entsprechende Ausweise, die der BfA im Original vorgelegt werden, nach Abschluß des Verfahrens an den Versicherten/Antragsteller zurückzusenden.

Ich habe darauf hingewiesen, daß dies auch für Kopien gelten müsse, die anstatt des Originals eingereicht werden. Die BfA hat meine Anregung aufgegriffen und ihre

Geschäftsanweisung dahingehend ergänzt, daß auch die Fotokopien an den Antragsteller zurückzusenden sind, wenn die Aktenvorgänge dem Archiv zugeleitet werden, also die erforderlichen Daten aus dem Ausweis erfaßt und im BfA-Vorgang des Versicherten gespeichert sind.

23 Unfallversicherung

23.1 Umsetzung des SGB VII

Im Gesetzgebungsverfahren zum SGB VII war es mein vorrangiges Ziel, den Versicherten so weit wie möglich in das Ermittlungs- bzw. Feststellungsverfahren einzubeziehen und die einzelnen Verfahrensschritte für ihn transparent zu gestalten sowie die Datenerhebung, -verarbeitung und -nutzung im einzelnen – orientiert am Maßstab der Verhältnismäßigkeit – normenklar festzulegen.

In meinem 16. TB habe ich insoweit eine befriedigende Bilanz meiner Bemühungen im Gesetzgebungsverfahren gezogen (vgl. 16. TB Nr. 23.1).

Zur Umsetzung des SGB VII hat das BMA im Juni 1998 dem Ausschuß für Arbeit und Sozialordnung des Deutschen Bundestages einen Bericht vorgelegt. Darin zog das BMA insgesamt eine positive Bilanz hinsichtlich der Qualität des Gutachterwesens, der Verbesserung der Prävention, der Informations- und Mitwirkungsrechte der Betroffenen sowie der Umsetzung des § 24 Abs. 1 SGB VII. Diesen Bericht, der anhand entsprechender Beiträge der Unfallversicherungsträger und ihrer Verbände erstellt wurde, konnte ich, soweit er datenschutzrelevante Themen ansprach, nur teilweise bestätigen.

23.1.1 Musterdienstanweisung HVBG

Die Gespräche mit dem HVBG über eine Musterdienstanweisung zur Umsetzung der SGB VII in die Praxis der Berufsgenossenschaften gestalteten sich als sehr schwierig und konnten Ende vergangenen Jahres nur unter Inkaufnahme mehrerer Kompromisse abgeschlossen werden.

Insbesondere zu folgenden Punkten wurde ein tragfähiger Kompromiß erreicht:

– **Zum Ersterhebungsgrundsatz**

  Zur Erhebung beim Betroffenen wurde im Kompromißwege u. a. festgehalten, daß die Datenerhebung beim Betroffenen grundsätzlich Vorrang vor der Datenerhebung bei anderen Personen oder Stellen (§ 67a Abs. 2 SGB X) hat. Dazu wird dem Versicherten für die Beantwortung des sog. Versichertenfragebogens eine Frist gesetzt. Sollte der Betroffene innerhalb dieser Frist nicht geantwortet haben, dürfen die Daten bei anderen erhoben werden. Trifft die Antwort innerhalb der drei Wochen ein, so ist vom Sachbearbeiter zu entscheiden, ob wegen unvollständiger, widersprüchlicher oder offensichtlich unrichtiger Angaben des Betroffenen im Rahmen des § 20 SGB X weitere Ermittlungen bei Dritten durchzuführen sind.

  In einer Klarstellung hierzu habe ich verdeutlicht, daß der Ersterhebungsgrundsatz nach meiner Auffassung die unmittelbare Erhebung beim Betroffenen und die Erhebung bei Dritten mit seiner Zustimmung umfaßt (§ 67a Abs. 2 Satz 1 SGB X i.V.m. § 60 Abs. 1 Nr. 1 SGB I). In diesem Zusammenhang habe ich auch darauf hingewiesen, daß Informationen über Erkrankungen und Vorerkrankungen zu Zwecken des Feststellungsverfahrens nicht unmittelbar beim Betroffenen erhoben werden sollen, sondern mit seiner Zustimmung bei Ärzten und Krankenkassen. Denn nach allgemeiner Lebenserfahrung ist davon auszugehen, daß er selbst die erforderlichen Angaben in der Regel nicht machen kann, jedenfalls nicht in dem durch die §§ 188, 203 SGB VII begrenzten Rahmen.

  Zum Abschluß der Verhandlungen hierüber wurden schließlich die folgenden Protokollnotizen vereinbart:

  „1. *Für die Erhebung beim Betroffenen (Nr. 5.2) ist die mögliche Abfrage von Vorerkrankungen konkret auf den zur Ermittlung anstehenden Sachverhalt auszurichten, so daß der Versicherte erkennen kann, daß nach offensichtlich für das Berufskrankheitenverfahren irrelevanten Vorerkrankungen nicht gefragt wird.*

  Bei Ziffer 1 gehe ich von unserer gemeinsamen Prämisse aus, daß Nachfragen an den Versicherten ohnehin nur erfolgen, wenn sachdienliche Auskünfte zu Vorerkrankungen zu erwarten sind.

  Diese Voraussetzungen liegen erfahrungsgemäß nur in Ausnahmefällen vor.“

  2. *Für die Erhebung bei Sozialversicherungsträgern sowie bei anderen Stellen und Personen (Nr. 5.3 und Nr. 5.4) ist es neben den in der Musterdienstanweisung aufgeführten Verfahren möglich und unschädlich, wenn die Erhebung mit ausdrücklicher Zustimmung des Betroffenen geschieht. Dies hält der BfD für die datenschutzrechtlich beste Lösung.“*

– **Zum Gutachterverfahren nach § 200 Abs. 2 SGB VII**

  = Qualifizierung des beratenden Arztes

  Einigkeit konnte zwar mit dem HVBG darüber erzielt werden, daß die Vorschrift des § 200 Abs. 2 SGB VII auch auf den beratenden Arzt anzuwenden ist, sofern er im Rahmen des Feststellungsverfahrens wie ein externer Gutachter eingesetzt wird. Präzisierende Abgrenzungskriterien, die den Sachbearbeitern eine Entscheidungshilfe für die Beurteilung bieten, ob der beratende Arzt als Gutachter tätig wird oder nicht, ließen sich dagegen noch nicht finden.

  In der Protokollnotiz hierzu heißt es deshalb ergänzend:

  „Die Abgrenzung zwischen dem beratenden Arzt und dem Gutachter ist eine abstrakte Zielformulierung, die in den nächsten Jahren möglichst anhand einer Reihe von Einzelfällen aus der Praxis weiter

konkretisiert werden sollte. Es besteht Einvernehmen, diese weitere Konkretisierung im gegenseitigen Abstimmungsprozeß zu suchen.“

= Zahl der den Betroffenen vorzuschlagenden Gutachter

Der HVBG hat hierzu zugestanden, daß die Anzahl der dem Betroffenen vorzuschlagenden Gutachter der Zahl der im einzelnen Versicherungsfall zur Verfügung stehenden Ärzte angemessen entsprechen soll, dem Betroffenen daher nicht wie *bisher „mindestens drei“,* sondern künftig *„drei oder mehr“* Gutachter vorzuschlagen sind. Aus meiner Sicht war diese Frage bereits ausführlich in diesem Sinne im Gesetzgebungsverfahren beraten worden.

= Gutachtervorschlagsrecht des Betroffenen

Das eigene Vorschlagsrecht der Versicherten wird in der Musterdienstanweisung des HVBG ebenso wenig erwähnt wie die Verpflichtung der Unfallversicherungsträger, den Versicherten auf sein Recht hinzuweisen, selbst geeignete Gutachter vorzuschlagen. Der HVBG war zwar bereit, ein Vorschlagsrecht des Versicherten im Grundsatz anzuerkennen, lehnte jedoch eine entsprechende Hinweispflicht der Berufsgenossenschaften mit der Begründung ab, daß dies infolge ungeeigneter Gutachtervorschläge der Versicherten in vielen Fällen zu Ausweitungen und Verzögerungen der Feststellungsverfahren führen würde.

In der Protokollnotiz vom 26. November 1998 heißt es dazu,

„... daß in einem Zeitraum von zwei bis drei Jahren, in dem die Musterdienstanweisung *mit den vorstehenden Erläuterungen auf ihre praktische Umsetzung hin von beiden Seiten betrachtet werden sollte, um sodann über gegebenenfalls notwendige Anpassungen Gespräche zu führen, im Rahmen eines Pilotprojektes abgeklärt werden könnte, ob und inwieweit der Hinweis in den Formularen auf ein aktives Vorschlagsrecht des Versicherten zu möglichen Verfahrensverzögerungen führt oder nicht.“*

= Folgen der Verletzung der Mitwirkungsobliegenheiten gem. §§ 60ff. SGB I

In die Musterdienstanweisung des HVBG war auf meinen Vorschlag in diesem Zusammenhang aufgenommen worden, daß dem Betroffenen, wenn er die seitens der Berufsgenossenschaft vorgeschlagenen Gutachter mit nachvollziehbarer Begründung ablehnt, nochmals weitere geeignete Gutachter vorgeschlagen werden. Das eigene Vorschlagsrecht des Versicherten war aber auch in diesem Zusammenhang unberücksichtigt geblieben.

Ich habe hierzu darauf hingewiesen, daß es z. B. bei der Konstellation zu Problemen führen kann, in der der Betroffene die ihm benannten Gutachter ablehnt und statt dessen selbst Gutachter vorschlägt; denn wenn seine Vorschläge sich als geeignet erweisen, kann die Ablehnung der Gutachtervorschläge der Berufsgenossenschaft durch ihn nicht als Verletzung seiner Mitwirkungsobliegenheiten gewertet und ihm deshalb eine Anerkennung nicht schon gem. § 66 SGB I verweigert werden.

– **Zu Einwilligung und Zustimmung**

= Die Musterdienstanweisung des HVBG wurde während der Verhandlungen in Kapitel 7 „Einwilligung des Betroffenen“ durch folgenden Satz ergänzt:

„Bestehen spezialgesetzliche Erhebungs- oder Übermittlungsbeschränkungen, können diese nicht durch Einwilligung durchbrochen werden.“

Beispielhafte Konkretisierungen für die Praxis ließen sich beim HVBG leider nicht durchsetzen.

Die Protokollnotizen enthalten hierzu folgende Formulierung:

„Die Einwilligung des Betroffenen (Nr. 7) ist nach einvernehmlicher Auffassung nur dann einzuholen, wenn es nicht bereits gesetzlich normierte Tatbestände für eine Datenverarbeitung oder -nutzung gibt; andererseits besteht gleichfalls Einvernehmen, daß eine Einwilligung trotz entsprechender Erlaubnistatbestände nicht schädlich ist, sondern gleichfalls rechtliche Wirkung in vom Gesetzgeber vorgegebenem Rahmen entfaltet. Einvernehmen besteht weiterhin darin, die abstrakt aufgeführten spezialgesetzlichen Erhebungs- oder Übermittlungsbeschränkungen, die nicht durch Einwilligung durchbrochen werden können, anhand konkreter Einzeltatbestände zukünftig im gegenseitigen Einvernehmen zu untermauern.“

= Mit Rücksicht darauf, daß der Entwurf der Musterdienstanweisung Ausführungen lediglich zur Einwilligung enthält, die nach dem SGB allein im Zusammenhang mit der Datenverarbeitung und -nutzung vorgesehen ist (§§ 67b und c SGB X), während im Zusammenhang mit der Datenerhebung das Rechtsinstitut der Zustimmung verwendet wird (§ 60 Abs. 1 Nr. 1 SGB I), hatte ich in den Verhandlungen eine entsprechende Ergänzung der Musterdienstanweisung dahin vorgeschlagen, daß die Regelungen zur Einwilligung entsprechend für die Zustimmung zur Datenerhebung bei Dritten gem. § 60 Abs. 1 Nr. 1 SGB I gelten.

Nach einem neuerlichen Vorstoß gehe ich davon aus, daß mir dies noch bestätigt werden wird.

Aufgrund der großen Zahl von Bürgereingaben kommt der Musterdienstanweisung des HVBG besondere Bedeutung zu. Sie hat zwar keine unmittelbare Rechtswirkung für die Mitgliedsberufsgenossenschaften. Da der HVBG aber aufgrund seiner Satzung für sich in Anspruch

nimmt, nicht lediglich beratend tätig zu werden, sondern aus seiner „Führungsfunktion“ (Grundsatz Nr. 4 der Satzung) heraus seinen Mitgliedern Handlungsleitlinien zu geben, fühlen sich die Mitgliedsberufsgenossenschaften im Sinne der satzungsmäßigen Verbandsdisziplin an diese gebunden (vgl. 16. TB Nr. 23.5). Das gilt grundsätzlich auch für die Musterdienstanweisung zum Datenschutz; nur in Ausnahmefällen sind mir bisher Dienstanweisungen von Berufsgenossenschaften begegnet, die in datenschutzrechtlichen Grundsatzfragen den Versicherten stärkere Rechtspositionen einräumten als dies in der Musterdienstanweisung des HVBG vorgesehen war. Inwieweit einzelne Berufsgenossenschaften die Verfahren im Zusammenhang mit Datenschutzkontrollen oder Bürgereingaben über den Einzelfall hinaus durch entsprechende Verbesserungen der Dienstanweisungen datenschutzfreundlicher gestalten werden, bleibt abzuwarten. Als nächsten Schritt habe ich mit dem HVBG vereinbart, daß die von den Berufsgenossenschaften verwendeten Formulare z. B. für die Anschreiben an die Versicherten, Versichertenfragebögen, Übermittlungsersuchen an Krankenkassen, sonstige Sozialleistungsträger und Ärzte in Abstimmung mit mir neu gefaßt werden sollen.

Anfang 1999 hat mir das BMA einen Vorentwurf eines Gesetzes zur Änderung des Sozialgesetzbuches zugeleitet. Ich werde nachdrücklich auf aus meiner Sicht im SGB VII und X gebotene gesetzliche Klarstellungen hinwirken, um die Probleme auszuräumen, auf welche die nachfolgend beschriebenen Defizite in der Verwaltungspraxis der Unfallversicherungsträger zurückzuführen sind.

23.1.2 Verträge zur Durchführung der Heilbehandlung nach § 34 SGB VII

Die Verbände der Unfallversicherungsträger schließen mit der Kassenärztlichen und Kassenzahnärztlichen Bundesvereinigung Verträge über die Durchführung der Heilbehandlung, die Vergütung der Ärzte und Zahnärzte sowie die Art und Weise der Abrechnung (§ 34 Abs. 3 SGB VII). Ein wesentlicher Anwendungsfall dieser Verträge ist das Durchgangsarztverfahren. Nach § 34 Abs. 3 Satz 2 SGB VII ist mir rechtzeitig vor Abschluß der Verträge Gelegenheit zur Stellungnahme zu geben, sofern in den Verträgen die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten geregelt werden soll.

Ich halte es im Rahmen dieses Verfahrens allerdings nicht für sachgerecht und auch nicht für eine „rechtzeitige“ Beteiligung im Sinne des § 34 Abs. 3 Satz 2 SGB VII, wenn mir ein solcher Vertragsentwurf erst ca. drei Wochen vor dem voraussichtlichen Inkrafttreten übersandt wird. Ich habe von einer förmlichen Beanstandung gem. § 81 Abs. 2 SGB X i.V.m. § 25 BDSG nur deshalb abgesehen, weil mir der HVBG versichert hat, das Inkrafttreten des Vertrages solange aufzuschieben, bis meine Stellungnahme vorliegt und ggf. berücksichtigt worden ist.

In meiner Stellungnahme zu diesem Entwurf habe ich gegenüber den Vertragsparteien insbesondere die Mehrfacherhebung der Angaben *„Unfallhergang und -zeitpunkt“* (nicht: Datum) aufgegriffen: Mit Ausnahme der in der Unfall-/Berufskrankheiten-Anzeige gemachten Angaben handelt es sich hierbei um die zeitversetzt gemachten eigenen Angaben des Versicherten gegenüber den Zahnärzten im Sinne des § 201 SGB VII, seinen vor- bzw. weiterbehandelnden Zahnärzten i.S.d. § 203 SGB VII und den Angaben im Ersterhebungsfragebogen. In diesem Kontext, der die Gefahr unzulässiger Mehrfacherhebungen birgt, ist die Datenerhebung bzw. -verarbeitung durch Zahnärzte gem. § 201 SGB VII i.V.m. § 34 SGB VII zu sehen.

Zu diesen verschiedenen Informationsquellen vertrete ich die Auffassung, daß neben dem Ersterhebungsfragebogen gem. § 67a Abs. 2 Satz 1 SGB X die Unfall- bzw. Berufskrankheiten-Anzeige nach § 193 SGB VII die primäre Informationsquelle sein muß, da die Anzeige im Hinblick auf die Beteiligung des Unternehmers und des Betriebs- oder Personalrats vom Gesetzgeber im Regelfall als die maßgebliche, gleichsam objektivierte Grundlage der Sachverhaltsfeststellung für den Unfallversicherungsträger vorgegeben ist.

Eine Erhebung der Angaben *„Unfallhergang und -zeitpunkt“* durch den Unfallversicherungsträger und Übermittlung durch den Zahnarzt auf der Grundlage des § 201 SGB VII ist m.E. nur dann zulässig,

– wenn die Unfallanzeige nicht vorliegt (vgl. § 193 Abs. 1 SGB VII) oder
– der Versicherte die Unvollständigkeit oder Unrichtigkeit der Anzeige geltend macht oder
– die Angaben des Versicherten im Ersterhebungsfragebogen unvollständig oder widersprüchlich sind.

Neben der verfassungsrechtlich am Maßstab der Verhältnismäßigkeit gebotenen engen Auslegung des § 201 SGB VII beruht meine Auffassung zudem darauf, daß wegen der zeitlichen Nähe zum Unfallgeschehen und der daraus resultierenden besonderen medizinischen Zustände – wie etwa Bewußtlosigkeit, starke Schmerzen oder Schockwirkungen – die Eignung und damit die Erforderlichkeit der Erhebung dieser Angaben für die Aufgabenerfüllung des Unfallversicherungsträgers in Frage gestellt ist.

Die Vertragsparteien berufen sich demgegenüber auf den Wortlaut des § 201 Abs. 1 Satz 2 SGB VII, wonach die Daten erhoben, gespeichert und übermittelt werden dürfen, die für ihre Entscheidung, eine Heilbehandlung nach § 34 SGB VII durchzuführen, maßgeblich waren.

Die Diskussion hierüber dauerte bei Redaktionsschluß noch an.

23.2 Datenschutz als Vorwand, Daten nicht zu erfragen

Häufig muß ich mich mit den meiner Kontrolle unterliegenden Stellen auseinandersetzen, weil sie zu viele Daten erheben und verarbeiten. Selten ist hingegen der Fall, daß unter ausdrücklicher Berufung auf den Datenschutz Daten erst gar nicht erhoben werden sollen, obwohl sie für Zwecke der Prävention oder – wie hier – für die Feststellung von Berufskrankheiten m. E. hilfreich wären.

Im Jahre 1995 habe ich mich mit der Erhebung, Verarbeitung und Nutzung der Daten befaßt, die in der Zentraldatei des HVBG für Zwecke der Feststellung von Erkrankungen, die wie Berufskrankheiten nach § 9 Abs. 2 SGB VII anzuerkennen sind, und für die Erfüllung von Präventionsaufgaben verwaltet werden. Im Zuge von Kontrollen bei Berufsgenossenschaften und des HVBG hatte ich festgestellt, daß in dem Fragebogen über die *„Anmeldung von Entschädigungsansprüchen nach § 551 Abs. 2 RVO“* (heute: § 9 Abs. 2 SGB VII) die Frage VII stets mit *„unbekannt“* ausgefüllt wurde oder gänzlich unbeantwortet blieb. Mit diesem Fragebogen übermitteln die Berufsgenossenschaften auf der Grundlage der bei ihnen eingegangenen Berufskrankheitenanzeigen die Daten, die erforderlich sind, um die Zentraldatei des HVBG korrekt führen zu können.

Die Frage VII in dem Fragebogen lautete:

„Sind im Unternehmen weitere Arbeitnehmer mit gleichen Arbeiten wie der/die Erkrankte beschäftigt und haben sich bei diesen ähnliche Krankheitserscheinungen gezeigt? Wenn ja, wann und welche?“

Zunächst räumte der HVBG ein, daß die konkrete Beantwortung der Frage VII im Hinblick auf den Zweck der Datei (§ 204 Abs. 1 Nr. 1 SGB VII), signifikante Häufungen und Tendenzen im Berufskrankheitengeschehen bzw. gefährdungsfreie und -arme Arbeitsbereiche frühzeitig erkennen und die einzelnen Unfallversicherungsträger bei der Prävention wirksam unterstützen zu können, grundsätzlich unverzichtbar sei. Dies gelte insbesondere im Hinblick darauf, daß eine Erkrankung nach § 9 Abs. 2 SGB VII im Einzelfall regelmäßig dann nicht wie eine Berufskrankheit nach Absatz 1 dieser Vorschrift anerkannt werden kann, wenn die Tatbestandsvoraussetzung *„durch besondere Einwirkungen verursacht, denen **bestimmte Personengruppen** durch ihre versicherte Tätigkeit in erheblich höherem Grade als die übrige Bevölkerung ausgesetzt sind“* (§ 9 Abs. 1 SGB VII) nicht zuverlässig geklärt ist. Auch können entsprechende Gefährdungsbereiche ohne die in Frage VII vorgesehenen Informationen kaum im Sinne der Einzel- und Generalprävention (§ 14 SGB VII) erkannt und beseitigt werden.

Zu meiner Überraschung wurde Frage VII in dem Fragebogen des HVBG für seine Mitgliedsberufsgenossenschaften unter Hinweis auf Datenschutzgründe schließlich ersatzlos gestrichen. BMA und HVBG begründeten dies damit, daß durch Frage VII Daten von Arbeitskollegen des Betroffenen ohne Rechtsgrundlage erhoben werden.

Dieser Beurteilung kann ich mich nicht anschließen. Insbesondere läßt sie sich nicht auf § 204 SGB VII stützen. Die Identifikation von Arbeitskollegen über die in Frage VII genannten Daten ist nur mit einem erheblichen Zusatzaufwand durch die Berufsgenossenschaften möglich und nicht durch den HVBG.

Ich habe dies dem BMA und dem HVBG mitgeteilt und betont, daß sie sich für die Streichung der Frage VII nicht auf Datenschutzgründe berufen können. Ich weise vorsorglich darauf hin, daß Gleiches für die hiermit korrespondierenden Fragen in den Anzeigeformularen für Berufskrankheiten gilt.

23.3 Arbeitsmedizinische Dienste

In meinem 16. TB (Nr. 23.2) hatte ich über die Neukodifizierung der Abschottung überbetrieblicher Arbeitsmedizinischer Dienste in § 24 SGB VII berichtet. Die Vorschrift erschien mir verheißungsvoll, zumal mir das BMA mitgeteilt hatte, sie dürfte *„dahin zu interpretieren sein, daß Arbeitsmedizinischer Dienst der Berufsgenossenschaft und die Berufsgenossenschaft als zwei unterschiedliche speichernde Stellen aufzufassen sind. Für die datenschutzrechtliche Trennung von Arbeitsmedizinischem Dienst und Berufsgenossenschaft spricht, daß ein ‚Übermitteln‘ von Daten nach § 67 Abs. 6 Satz 3 SGB X nur an einen Dritten erfolgen kann.“*

Leider hat sich das BMA inzwischen von seiner früheren Auffassung distanziert, ohne auf seine damalige Argumentation einzugehen.

Aus dem in § 24 Abs. 1 Satz 2 SGB VII verwandten Terminus „übermitteln“ ergibt sich m.E. das Ziel des Gesetzgebers, eine von dem bzw. den errichtenden Unfallversicherungsträger(n) datenschutzrechtlich gesonderte „speichernde Stelle“ im Sinne von § 67 Abs. 9 Satz 1 SGB X zu schaffen. Denn „Übermitteln“ setzt einen Dritten als Empfänger voraus. Nach meiner Auffassung schließt allerdings der Gesetzeswortlaut auch eine Einrichtung der Arbeitsmedizinischen Dienste unter Zuordnung zu einer Berufsgenossenschaft bei gesicherter organisatorischer, personeller und räumlicher Abschottung nicht aus. Jenseits sprachlicher Angleichungen liegen die wesentlichen Änderungen des § 24 SGB VII gegenüber § 719a RVO, der Vorgänger-Vorschrift, in der Ergänzung der datenschutzrechtlichen Maßgaben in den neuen Sätzen 2 bis 4 von § 24 Abs. 1 SGB VII. Offenkundiges Ziel des Gesetzgebers ist es, die datenschutzrechtliche Eigenständigkeit und Unabhängigkeit überbetrieblicher Arbeitsmedizinischer Dienste als selbständige Einrichtung zu sichern.

Der datenschutzrechtlichen Selbständigkeit dieser Dienste gegenüber den Berufsgenossenschaften kommt wesentliche Bedeutung zu. Entgegen den verschiedentlich geäußerten Bedenken ist die Eigenständigkeit der Arbeitsmedizinischen Dienste auch praktikabel. Ich habe dies in einer ausführlichen rechtlichen Stellungnahme ausgearbeitet und hoffe, in weiteren Gesprächen mit dem BMA und dem HVBG eine den offenbaren Absichten des Gesetzgebers besser gerecht werdende Lösung für die Praxis zu finden.

23.4 Gutachtertätigkeit in der gesetzlichen Unfallversicherung

Der Einsatz von durch Unfallversicherungsträger ausgewählten Gutachtern wird immer wieder öffentlich diskutiert. Insbesondere durch Eingaben werde ich mit Problemen des Gutachtereinsatzes in Feststellungsverfahren der Unfallversicherungsträger konfrontiert.

Im Rahmen meiner Aufgaben habe ich beim Einsatz von Gutachtern die Einhaltung datenschutzrechtlicher Vorschriften in folgenden Verfahrensschritten zu kontrollieren:

– Erhebung personenbezogener Daten des Gutachters für die Erstellung und Führung von Gutachterlisten und -dateien (§§ 199 Abs. 1 SGB VII, 67a Abs. 1 SGB X),
– Verarbeitung, Nutzung und Speicherung dieser Daten (§§ 199 Abs. 1 SGB VII, 67b, 67c SGB X),
– Übermittlung der Gutachterdaten an den Versicherten zur Ausübung des Auswahlrechts (§§ 199 Abs. 1 SGB VII, 69 Abs. 1 SGB X i.V.m. § 200 Abs. 2 SGB VII),
– Übermittlung der Sozialdaten der Versicherten an den Gutachter (§ 69 Abs. 1 Nr. 1 SGB X i.V.m. § 200 Abs. 2 SGB VII).

Diese datenschutzrechtlichen Bezüge werden von einzelnen Berufsgenossenschaften in Frage gestellt und damit meine Befugnis, die inhaltliche Ausgestaltung der einzelnen Verfahrensschritte, insbesondere die Gutachterauswahl, zu kontrollieren. Begründet wird das mit der umfassenden Amtsermittlungspflicht der Unfallversicherungsträger nach §§ 20, 21 SGB X. Diese Argumentation übersieht indessen den Vorrang der Datenschutzvorschriften der § 67ff SGB X i.V.m. § 60 SGB I gegenüber den genannten Verfahrensregelungen (§ 37 SGB I). Der Einsatz von Gutachtern in unfallversicherungsrechtlichen Feststellungsverfahren beurteilt sich danach gem. § 37 Satz 3 SGB I nach Maßgabe der Vorschriften des zweiten Kapitels des SGB X jeweils i.V.m. § 199 SGB VII.

Nach § 81 Abs. 2 SGB X i.V.m. § 24 BDSG habe ich bei den öffentlichen Stellen des Bundes die Einhaltung der Vorschriften über den Datenschutz zu kontrollieren. Für die Erforderlichkeit der Speicherung und Übermittlung von Gutachterdaten an Versicherte einerseits und der Übermittlung von Versichertendaten an Gutachter andererseits ist auch wesentlich, ob der Gutachter geeignet ist. Dabei beschränke ich mich auf eine Plausibilitätsprüfung. Stelle ich im Rahmen einer Kontrolle Anhaltspunkte für Auffälligkeiten oder offensichtliche Widersprüche fest, z. B. wenn in einer Gutachterdatei für Knochenerkrankungen ein Augenarzt geführt wird, bin ich bemüht, die Diskrepanz ggf. auch unter Einschaltung der Aufsichtsbehörden aufzuklären.

Daß sich bei der Überprüfung der Erforderlichkeit der Datenverwendung im aufgezeigten Rahmen Berührungen oder möglicherweise auch Überschneidungen mit den Aufgaben der Aufsichtsbehörde – wenn auch nur auf dem genannten engen Sektor – ergeben, liegt in der Natur der Sache.

In dem hier erörterten Zusammenhang ist auch von besonderer Bedeutung, daß mich der Ausschuß für Arbeit und Sozialordnung des Deutschen Bundestages gebeten hat, ihm über die Umsetzung des SGB VII durch die Unfallversicherungsträger unter besonderer Berücksichtigung der Handhabung des Gutachterverfahrens gem. § 200 Abs. 2 SGB VII zu berichten. Der Deutsche Bundestag hatte die bereits von mir im 15. TB (Nr. 10.8) dargestellte Problematik der Gutachterauswahl teilweise aufgegriffen und mit der Einfügung des § 200 Abs. 2 SGB VII umgesetzt. Damit sollen die Rechte der Versicherten im Verwaltungsverfahren insbesondere das Recht auf informationelle Selbstbestimmung und auf Mitwirkung gestärkt und die Transparenz des Verfahrens verbessert werden.

Zusätzlich zu der schon bislang nach § 76 Abs. 2 Nr. 1 SGB X bestehenden Pflicht der Unfallversicherungsträger, die Versicherten auf ihr Recht hinzuweisen, der Übermittlung von Sozialdaten an einen Gutachter zu widersprechen, haben sie nach § 200 Abs. 2 SGB VII dem Versicherten grundsätzlich mehrere Gutachter zur Auswahl vorzuschlagen. Und die Versicherten haben das Recht, selbst einen oder mehrere Gutachter vorzuschlagen. Dieses Recht ist zwar nicht ausdrücklich in § 200 Abs. 2 SGB VII benannt, ergibt sich aber aus der ratio legis dieser Vorschrift, insbesondere der Stärkung der Mitwirkungsrechte der Versicherten.

Darüber hinaus zielt meine Beratung der datenverarbeitenden Stellen naturgemäß nicht nur auf die korrekte Beachtung der Vorschriften, sondern auch darauf, die bestehenden Gestaltungsspielräume nicht zu Lasten der Betroffenen zu nutzen. In diese Richtung zielt auch § 97 Abs. 1 SGB X, wonach in den Fällen, in denen ein Leistungsträger von einem Dritten Aufgaben wahrnehmen lassen kann, sichergestellt sein muß, daß der Dritte die Gewähr für eine sachgerechte, die Rechte und Interessen des Betroffenen wahrende Erfüllung der Aufgaben bietet.

Weitere Probleme im Zusammenhang mit dem Einsatz von Gutachtern im Feststellungsverfahren habe ich in den nachfolgenden Kapiteln beschrieben.

23.4.1 Hinweise auf das Auswahl- und Vorschlagsrecht des Versicherten

Der noch aus dem römischen Recht stammende zivilrechtliche Grundsatz, daß sich jeder selbst um die ihm zustehenden Rechte zu kümmern hat, hat gerade im Sozialrecht keine Berechtigung und würde auch zynisch wirken. Vor allem im Unfallversicherungsrecht stehen sich nicht gleichberechtigte Vertragspartner gegenüber. Vielmehr stellt ein Einzelner, der häufig bereits durch langwierige Krankheit existentiell geschwächt ist, einen Anspruch gegen den wirtschaftlich und auch personell starken Unfallversicherungsträger. Wegen dieses Ungleichgewichts kommen Aufklärungs-, Beratungs- und Hinweispflichten gegenüber dem Versicherten eine besondere Bedeutung zu (§§ 13, 14, 15 SGB I).

Diese Ausgangsposition führt m. E. zu folgenden Schlußfolgerungen beim Einsatz von Gutachtern:

– Es kann den Fall geben, daß der Versicherte eine Auswahl unter mehreren von der Berufsgenossenschaft benannten Gutachtern nur dann treffen kann, wenn er zusätzliche Informationen zum Gutachter erhält. Ansonsten könnte er von seinem Widerspruchs-

recht nach § 200 Abs. 2 SGB VII i.V.m. § 76 Abs. 2 SGB X keinen sachgerechten, sondern nur einen Gebrauch „ins Blaue hinein“ machen. Insofern ist m. E. der Versicherte auf Wunsch über den ausgewählten Gutachter zu informieren.

– Die Unfallversicherungsträger sollten den Versicherten im Rahmen einer Begutachtung darauf hinweisen, daß er selbst einen Gutachter vorschlagen kann. Das trägt der gebotenen Transparenz des Verfahrens am besten Rechnung. Das Gutachtervorschlagsrecht der Versicherten wird nur noch in Ausnahmefällen von einzelnen Berufsgenossenschaften in Frage gestellt. Anders sieht es jedoch insoweit mit der Hinweispflicht gegenüber dem Versicherten auf dessen Gutachtervorschlagsrecht aus. Sowohl der HVBG als auch die von mir bisher darauf angesprochenen Berufsgenossenschaften lehnen einen Hinweis mit der Begründung ab, daß das Vorschlagsrecht der Versicherten nicht in das Gesetz aufgenommen worden sei und die entsprechenden Ausführungen in der Ausschußbegründung nur als unverbindliche Anregungen zu werten seien. Die Berufsgenossenschaften haben große Bedenken, daß die Versicherten ausschließlich ihre eigenen Hausärzte benennen würden, die im Regelfall nicht über die erforderlichen Fachkenntnisse verfügen. Ich gehe daher davon aus, daß die Versicherten auch nach dem Inkrafttreten des § 200 Abs. 2 SGB VII von keiner Berufsgenossenschaft auf ihr Recht, eigene Gutachter vorzuschlagen, hingewiesen werden.

Die Einwände und Befürchtungen der Berufsgenossenschaften halte ich nicht für begründet. Es besteht die Gefahr, daß das Vorschlagsrecht – mangels Kenntnis des Versicherten – überhaupt nicht wahrgenommen werden kann und so ins Leere läuft. Nach meiner Ansicht muß für den Regelfall vorausgesetzt werden, daß der Betroffene über ihn betreffende Verfahrensschritte informiert werden will, um dann zu entscheiden, ob und in welchem Umfang er von seinen Mitwirkungsrechten Gebrauch machen will. Diese Sichtweise entspricht den Grundsätzen der Transparenz des Verfahrens und wird offenbar auch vom BMA grundsätzlich geteilt. Nach dessen Auffassung hat eine Beratung des Betroffenen auch ohne Nachfrage durch den Sozialleistungsträger zu erfolgen, falls die Ausübung eines Rechts durch den Betroffenen auf der Hand liegt, wenn er diese Möglichkeit erkennt (vgl. die vom BMA herausgegebene „Übersicht über das Sozialrecht“, 5. Auflage, Stand: 1. Januar 1998, Seite 35, Anm. 12).

Wegen der starken Vorbehalte der Berufsgenossenschaften gegen einen Hinweis auf ein Vorschlagsrecht habe ich im Rahmen meiner Verhandlungen über eine Musterdienstanweisung für den Datenschutz (s. o. Nr. 23.1.1) als Kompromißlösung einem Pilotprojekt zugestimmt. Danach sollen zunächst von ein oder zwei Berufsgenossenschaften entsprechende Hinweise an die Versicherten gegeben werden, um Erfahrungen darüber zu sammeln, in welchem Umfang und mit welchen Ergebnissen vom Vorschlagsrecht Gebrauch gemacht wird. Das Pilotprojekt soll darüber Auskunft geben, ob die Besorgnis begründet ist, daß das Feststellungsverfahren infolge des Hinweises auf das Vorschlagsrecht und den Vorschlag nicht geeigneter Gutachter durch die Versicherten im Vergleich zu dem bisher in § 200 Abs. 2 SGB VII geregelten Verfahren zu erheblichen zeitlichen Verzögerungen und entsprechendem Verwaltungsaufwand führt. Ich gehe zwar davon aus, daß ich an der Konzeption und der Begleitung des Pilotverfahrens und der Auswahl der beteiligten Berufsgenossenschaften maßgeblich beteiligt sein werde, wie an der Auswertung seiner Ergebnisse. Diese dürften aber erst nach einer Laufzeit von 2 bis 3 Jahren verwertbar vorliegen. Eine eindeutige gesetzliche Regelung des Gutachtervorschlagsrechts des Versicherten und der entsprechenden Hinweispflicht der Unfallversicherungsträger erscheint mir nach allem geboten, um auch insoweit so schnell wie möglich Rechtssicherheit für alle Betroffenen herzustellen.

23.4.2 Qualifizierung des beratenden Arztes

Die Unfallversicherungsträger beschäftigen auch sog. beratende Ärzte, die insbesondere zur Unterstützung bei der Überwachung des Heilverfahrens aber auch der Sachbearbeiter im Feststellungsverfahren zur Beratung und Erläuterung schwieriger medizinischer Sachverhalte oder atypischer Fallgestaltungen eingesetzt werden. Sie sind häufig wie Mitarbeiter der Verwaltung zu sehen und gehören somit zur speichernden Stelle. Die Weitergabe medizinischer Unterlagen eines Versicherten an einen beratenden Arzt ist nur dann eine Datenübermittlung, wenn dieser als Dritter nach § 67 Abs. 10 SGB X anzusehen ist. Eine Datenübermittlung ist jedoch Voraussetzung für das Recht des Versicherten, der Weitergabe seiner Daten im Zusammenhang mit einer Begutachtung nach § 76 Abs. 2 SGB X zu widersprechen und nach § 200 Abs. 2 SGB VII unter mehreren Gutachtern auszuwählen bzw. selbst Gutachter vorzuschlagen.

Wird nun ein beratender Arzt wie ein externer Gutachter tätig, halte ich es aus Gründen der Rechtssicherheit und, um Umgehungstatbestände zum Nachteil der Versicherten zu verhindern, für zwingend, den beratenden Arzt als Dritten nach § 67 Abs. 10 SGB X anzusehen, damit § 200 Abs. 2 SGB VII i.V.m. § 76 Abs. 2 SGB X von den Versicherten angewandt werden kann. Das entspricht dem Willen des Gesetzgebers, der in der Begründung zum Gesetzesentwurf davon ausgegangen ist, daß ein Auswahlrecht immer dann eingreift, *„wenn ein medizinisches Gutachten eingeholt werden muß“* (BT-Drs. 13/4853 vom 12. Juni 1996, S. 13).

Insoweit habe ich in meinen Beratungen zu einem Entwurf einer Musterdienstanweisung für den Datenschutz Einvernehmen mit dem HVBG erzielt. Für die Anwendbarkeit des § 200 Abs. 2 SGB VII stellt sich damit indessen die weitere Frage, in welchen Fällen der beratende Arzt wie ein externer Gutachter tätig wird. Hierüber habe ich mit den Berufsgenossenschaften und dem HVBG bislang keinen Konsens erzielen können (s. o. Nr. 23.1.1).

Kriterien für die Unterscheidung „beratender Arzt“ oder „Gutachter“ können m.E. nur aus der Praxis abgeleitet

werden. Aus meinen bisherigen Erfahrungen könnte dabei von maßgeblicher Bedeutung sein:

– Der beratende Arzt gibt seine Stellungnahme nach einer körperlichen Untersuchung des Versicherten ab.

– Die Stellungnahme eines beratenden Arztes erfolgt zwar aufgrund der Aktenlage, schließt aber eine sachverständige Beurteilung zu Zusammenhangsfragen im Rahmen der haftungsbegründenden bzw. haftungsausfüllenden Kausalität ein. Das ist insbesondere dann der Fall, wenn Aussagen dazu gemacht werden, ob die berufliche Tätigkeit die schädigende Einwirkung zur Folge hatte (haftungsbegründende Kausalität) und/oder die Einwirkung die Erkrankung verursacht hat (haftungsausfüllende Kausalität). Das umfaßt auch Stellungnahmen zur Höhe der Erwerbsminderung oder zu einem bereits vorliegenden Gutachten, da auch damit eine Feststellung über den kausalen Zusammenhang bei einer Berufskrankheit getroffen wird.

– Eine Aussage des Arztes erfolgt im Rahmen des Feststellungsverfahrens zu den Grenzen der Mitwirkungspflicht nach § 65 Abs. 2 SGB I. Der Wortlaut der Vorschrift des § 76 Abs. 2 SGB X, auf den § 200 Abs. 2 SGB VII verweist, steht einer Anwendbarkeit nicht entgegen, da eine Begutachtung zur Feststellung der Grenzen der Mitwirkungspflichten ebenfalls *„wegen der Erbringung von Sozialleistungen“* vorgenommen wird.

Bei der Begutachtung durch einen beratenden Arzt stellt sich jedoch die Frage, ob er wegen der engen wirtschaftlichen Verflechtung mit der Berufsgenossenschaft von dieser überhaupt als unabhängiger Gutachter geführt und vorgeschlagen werden sollte.

23.4.3 Umgehung der Gutachterregelung durch die Berufskrankheiten-Verordnung

Das Feststellungs- und Anerkennungsverfahren für Berufskrankheiten liegt in der ausschließlichen Verantwortung der Unfallversicherungsträger. Um jedoch die speziellen Erfahrungen der Gewerbeärzte, die regelmäßig für den medizinischen Arbeitsschutz zuständig sind, für die Sachverhaltsaufklärung zu nutzen, sieht die Berufskrankheiten-Verordnung (BKV) die Mitwirkung dieser Stellen durch obligatorische Unterrichtung und weitere Beteiligung vor.

So können nach § 4 Abs. 3 Satz 2 BKV die für den medizinischen Arbeitsschutz zuständigen Stellen ergänzende, die Unfallversicherungsträger bindende, Beweiserhebungen vorschlagen. Hierzu zählt auch die Vergabe von Zusammenhangsgutachten. Aus diesem für den Unfallversicherungsträger bindenden Vorschlag der zuständigen Arbeitsschutzstelle, wird von den Beteiligten, wie ich anhand mehrerer Einzelfälle festgestellt habe, häufig geschlossen, daß auch ein in dem Vorschlag an den Unfallversicherungsträger gegebenenfalls enthaltener konkreter Gutachtervorschlag für diesen verbindlich ist.

So hat sich ein durch Holzschutzmittel erkrankter Versicherter in einer Eingabe an mich gewandt, über den in einem Verfahren auf Anerkennung einer Berufskrankheit bereits vier Gutachten durch die Berufsgenossenschaft eingeholt wurden. Alle Gutachter bestätigten das Vorliegen einer Berufskrankheit und eine Erwerbsminderung von über 20%. Die Berufsgenossenschaft hatte daher dem Versicherten bereits die Anerkennung in Aussicht gestellt und die rückwirkende Zahlung einer Teilrente veranlaßt. Sie teilte ihm mit, sie müsse ihren Entscheidungsvorschlag nur noch gem. § 4 Abs. 3 Satz 1 BKV dem zuständigen Gewerbearzt vorlegen. Da dieser in seinem Gutachten zu dem Ergebnis kam, daß eine Berufskrankheit nicht vorliege, hat er der Berufsgenossenschaft nach § 4 Abs. 3 Satz 2 BKV vorgeschlagen, ein weiteres Zusammenhangsgutachten bei einem von ihm benannten Gutachter in Auftrag zu geben. Die Berufsgenossenschaft erklärte sich an den Gutachtervorschlag des zuständigen Gewerbearztes auch dann noch gebunden, als der Versicherte sie auf seine Rechte nach § 200 Abs. 2 SGB VII hingewiesen hatte.

Mir sind noch mehrere andere Fälle bekannt geworden, in denen Berufsgenossenschaften Gutachtervorschläge des zuständigen Gewerbearztes übernommen haben, ohne dem Betroffenen auch in diesem Zusammenhang das Recht einzuräumen, unter mehreren vorgeschlagenen Gutachtern auszuwählen oder selbst Gutachter vorzuschlagen.

Diese Verfahrensweise widerspricht dem Sinn und Zweck des § 200 Abs. 2 SGB VII. Mit dieser Vorschrift soll eine Verbesserung der Transparenz des Verfahrens und eine Stärkung der Mitwirkungsrechte der Versicherten im gesamten unfallversicherungsrechtlichen Feststellungsverfahren erreicht werden. Es gibt nach meiner Auffassung für die Gewährung der Rechte nach § 200 Abs. 2 SGB VII keinen sachlichen Grund danach zu differenzieren, ob das Gutachten von dem Unfallversicherungsträger aufgrund eigener Entscheidung oder aufgrund eines verbindlichen Vorschlags der für den medizinischen Arbeitsschutz zuständigen Stelle in Auftrag gegeben wird.

Ich habe dem BMA meine Auffassung mitgeteilt und angeregt, § 4 Abs. 3 BKV zur Klarstellung um den Satz „§ 200 Abs. 2 SGB VII bleibt unberührt.“ zu ergänzen.

Meine Auffassung, daß die für den medizinischen Arbeitsschutz zuständigen Stellen im Rahmen ihres Vorschlagsrechts über ergänzende Beweiserhebungen nach § 4 Abs. 3 Satz 2 BKV den Unfallversicherungsträger nicht verpflichten können, einen bestimmten Gutachter zu beauftragen, wird vom BMA geteilt. Es hält eine Klarstellung in § 4 Abs. 3 BKV gleichwohl nicht für erforderlich, da § 200 Abs. 2 SGB VII als höherrangiges Recht von einer Verordnungsbestimmung nicht abgeändert oder eingeschränkt werden könne.

Ich halte – schon aufgrund meiner bisherigen Erfahrungen – einen klarstellenden Hinweis für geboten und habe dies dem BMA mitgeteilt.

23.4.4 Problematische Einzelfälle im Zusammenhang mit der Gutachterregelung nach § 200 Abs. 2 SGB VII

23.4.4.1 Übersendung medizinischer Daten eines Versicherten gegen dessen ausdrücklichen Widerspruch an einen Gutachter

Ein Versicherter beantragte bei der Verwaltungs-Berufsgenossenschaft die Anerkennung einer Berufskrankheit. Bereits zu Beginn wie auch im weiteren Verlauf des Verfahrens hatte er betont, daß seine medizinischen Daten nur mit seiner ausdrücklichen Zustimmung weitergegeben werden dürften.

Im Rahmen des Feststellungsverfahrens schlug die Berufsgenossenschaft eine Blutuntersuchung bei einem naturwissenschaftlichen Sachverständigen vor. Da der Versicherte jedoch bereits auf eigene Initiative Blutuntersuchungen hatte machen lassen, stellte er diese zur Verfügung. In einer anschließenden Besprechung mit der Berufsgenossenschaft, u. a. auch zur Frage der Begutachtung, schlug er einen Gutachter vor.

Kurz darauf gab die Berufsgenossenschaft die vom Versicherten eingereichten Blutanalysen an den von ihr bereits für die Befunderhebung vorgeschlagenen Sachverständigen weiter und bat um die Beurteilung der Ergebnisse der Blutproben. Dessen Stellungnahme hält die Berufsgenossenschaft nicht für ein Gutachten im Sinne von § 200 Abs. 2 SGB VII, da der dort genannte Gutachtenauftrag Fälle betreffe, *„die das Vertrauen des Versicherten besonders berühren, vor allem bei Begutachtungen mit Untersuchungen oder nach Aktenlage“.* Diese Argumentation überzeugt mich nicht. Allein eine Bezeichnung eines Gutachtens als „Stellungnahme“ oder „Auswertung“ kann nicht ausreichen, um die Anwendung gesetzlicher Vorschriften auszuschließen. Grundsätzlich ist jede eigenständige Ursachenbewertung zur Feststellung einer Berufskrankheit durch einen medizinisch-wissenschaftlichen Sachverständigen ein Gutachten.

Die Berufsgenossenschaft hielt dennoch an Ihrer Auffassung fest, daß kein Gutachten vorliege. Sie begründete das in einer abschließenden Stellungnahme damit, daß die Datenübermittlung in einem Ermittlungsschritt erfolgte, der einer Begutachtung vorausgehe: Es sollte zuerst festgestellt werden, ob die Blutwerte einen Hinweis auf eine Exposition mit bestimmten Gefahrstoffen aufwiesen.

Auch diese Begründung überzeugt mich nicht. Eine Begutachtung i.S.d. § 200 Abs. 2 SGB VII liegt nicht nur vor, wenn es um die Klärung der haftungsausfüllenden Kausalität, sondern auch der haftungsbegründenden Kausalität geht. Denn § 200 Abs. 2 SGB VII verweist auf § 76 Abs. 2 SGB X , der das Widerspruchsrecht an die Datenübermittlung *„wegen der Erbringung von Sozialleistungen“* knüpft.

Die Übermittlung von medizinischen Daten des Versicherten an den naturwissenschaftlichen Sachverständigen habe ich sowohl angesichts des fehlenden Hinweises auf ein Widerspruchsrecht, des fehlenden Vorschlags mehrerer Gutachter zur Auswahl und der Nichtberücksichtigung des Gutachtervorschlags des Petenten als auch bezüglich der Datenübermittlung gegen den Widerspruch des Petenten wegen Verstoßes gegen § 200 Abs. 2 SGB VII i.V.m. § 76 Abs. 2 SGB X **beanstandet**.

Zu meinem Bedauern hat sich die Berufsgenossenschaft meiner Auffassung weder angeschlossen noch ist sie meiner Empfehlung nachgekommen, den Bescheid aufzuheben. Der Versicherte hat mir dazu vielmehr mitgeteilt, die Verwaltungs-Berufsgenossenschaft habe in dem nunmehr anhängigen sozialgerichtlichen Verfahren vorgetragen, sie halte den Bescheid entgegen meiner Auffassung für rechtmäßig. Auch für vergleichbare Fälle wurde keine andere Verfahrensweise in Aussicht gestellt, so daß weitere Gespräche in dieser Angelegenheit nicht aussichtsreich erscheinen.

Ich habe den Fall dem Bundesversicherungsamt zur fachaufsichtlichen Prüfung übermittelt.

23.4.4.2 Mißachtung von Gutachtervorschlägen einer Versicherten und Entscheidung wegen mangelnder Mitwirkung

Zur Feststellung der haftungsbegründenden Kausalität hielt die Verwaltungs-Berufsgenossenschaft eine Untersuchung und eine Begutachtung zu der Frage für erforderlich, welchen Gefahrstoffen eine Versicherte ausgesetzt war. Sie schlug ihr drei Gutachter zur Auswahl vor, die diese bereits zu Beginn des Verfahrens abgelehnt hatte, und wies ausdrücklich – wie schon mehrfach zuvor in dem gesamten Schriftwechsel – auf die Mitwirkungspflichten der Versicherten und die Folgen der fehlenden Mitwirkung nach § 66 SGB I – ggf. Ablehnung der Anerkennung – hin.

Die Versicherte lehnte weiterhin die von der Berufsgenossenschaft vorgeschlagenen Gutachter ab und benannte in demselben Schreiben vier andere Gutachter.

In diesem Verfahrensstadium wandte sie sich an mich. Nachdem ich mit Schreiben vom 25. März 1998 die Berufsgenossenschaft um Stellungnahme gebeten hatte, lehnte diese den Antrag der Versicherten mit Bescheid vom 17. April 1998 mit der Begründung ab, daß bei Messungen an den Arbeitsplätzen keine Schadstoffbelastungen festgestellt worden waren. Zu der zuvor für erforderlich gehaltenen Begutachtung kam es nicht.

In einer Stellungnahme mir gegenüber und auch in der Begründung des Widerspruchsbescheides stellte die Verwaltungs-Berufsgenossenschaft klar, daß eine Entscheidung nach § 66 SGB I wegen fehlender Mitwirkung der Versicherten getroffen worden war. Die von ihr vorgeschlagenen Gutachter seien nicht geeignet gewesen. Die Gründe dieser Entscheidung habe sie der Petentin nicht mitteilen müssen.

Diese Auffassung wird in keiner Weise den Rechten der Versicherten nach § 200 Abs. 2 SGB VII gerecht. Zwar ist der Vorschlag des Versicherten für die Berufsgenossenschaft nicht verbindlich. Aber die Nichtgewährung dieses Rechtes durch die Ablehnung des bzw. der Gutachter bedarf einer konkreten und nachvollziehbaren Begründung. Das entspricht nicht nur dem Recht des Ver-

sicherten auf Transparenz des Verfahrens, sondern auch der Intention des § 200 Abs. 2 SGB VII, die Mitwirkungsrechte der Versicherten zu stärken.

Vor allem im Hinblick auf die Rechtsfolgen des § 66 SGB I ist ein begründeter Hinweis darauf geboten, daß ein vom Versicherten vorgeschlagener Gutachter für nicht geeignet erachtet wird. Diese Rechtsfolgen können in den Fällen, in denen die Berufsgenossenschaften dem Vorschlag des Versicherten nicht folgen, nicht ohne weiteres eintreten. Die Ausübung eines Rechtes kann für den Versicherten nicht zur Folge haben, daß sein Antrag wegen fehlender Mitwirkung abgelehnt wird.

Die Bewertung, die Versicherte habe gegen die Mitwirkungspflichten verstoßen, habe ich wegen der Verletzung des Gutachtervorschlagsrechts der Versicherten als Verstoß gegen § 200 Abs. 2 SGB VII **beanstandet**.

Darüber hinaus hatte die Berufsgenossenschaft ihre Bewertung der Qualifikation der von der Versicherten als Gutachter vorgeschlagenen Ärzte nicht offengelegt. In einem Schreiben habe ich der Berufsgenossenschaft mitgeteilt, daß die vorgeschlagenen Ärzte nach meiner Kenntnis namhafte Wissenschaftler seien. Daraufhin hat die Berufsgenossenschaft mir lediglich geantwortet, die Bewertung der Eignung von Gutachtern liege nicht in meinem Aufgabenbereich. Das stellt nicht nur eine Verletzung der Unterstützungspflichten nach § 81 Abs. 2 SGB X i.V.m. § 24 Abs. 4 Satz 1 und Satz 2 Nr. 1 BDSG dar, sondern ist auch eine sachlich unzutreffende Argumentation, weil sich nur durch die Beantwortung dieser Fragen die Begründung für eine Ablehnung der vorgeschlagenen Gutachter überprüfen läßt. Dazu habe ich die Verwaltungs-Berufsgenossenschaft erneut um Stellungnahme gebeten, die bei Redaktionsschluß noch nicht vorlag.

Auch zu diesem Fall habe ich das Bundesversicherungsamt informiert.

23.4.4.3 Übersendung medizinischer Daten eines Versicherten ohne dessen Wissen an einen beratenden Arzt

In einem Verfahren auf Feststellung einer Berufskrankheit bei der Berufsgenossenschaft der chemischen Industrie war eine Begutachtung eines Versicherten in Auftrag gegeben worden. Der Gutachter wurde in einem den datenschutzrechtlichen Vorgaben entsprechenden Verfahren beauftragt. Nachdem er zugunsten des Versicherten Aussagen getroffen hatte, bat die Berufsgenossenschaft einen beratenden Arzt um Stellungnahme nach Lage der Akten, ob dem Gutachten gefolgt werden könne. Dabei wurde der Versicherte weder auf sein Widerspruchsrecht in die Datenübermittlung noch auf sein eigenes Vorschlagsrecht hingewiesen und ihm wurden auch keine Gutachter zur Auswahl benannt.

Die Berufsgenossenschaft hält die Weitergabe der medizinischen Daten nicht für eine Datenübermittlung, da der Arzt wegen eines ständigen Vertragsverhältnisses kein Dritter im Sinne des § 67 Abs. 10 SGB X sei. In seiner Funktion als beratender Arzt sei er mit einer Stellungnahme nach Lage der Akten nicht aber mit der Erstellung eines Gutachtens beauftragt worden (s. auch Nr. 23.4.2).

Die Bewertung der Berufsgenossenschaft, die Weitergabe der medizinischen Daten sei keine Datenübermittlung ist nicht zutreffend. Für mich ist vielmehr entscheidend, daß eine Übermittlung an einen Sachverständigen erfolgte, der wie ein externer Gutachter eine eigenständige Bewertung vornimmt. Ein beratender Arzt ist aber nur dann als Teil der speichernden Stelle im Sinne des § 67 Abs. 10 SGB X anzusehen, wenn er – quasi als Abteilung – die Funktion der speichernden Stelle wahrnimmt. Das trifft jedoch auf einen beratenden Arzt nicht zu, der als Sachverständiger eine eigenständige Bewertung abgibt.

Die Stellungnahme zu der Frage, ob dem bereits vorliegenden Gutachten gefolgt werden könne, ist auch ein Gutachten im Sinne des § 200 Abs. 2 SGB VII. Wie bereits dargelegt (s. o. Nr. 23.4.4.1), kann allein die Benennung als Stellungnahme nicht ausreichen, um gesetzliche Vorschriften für anwendbar bzw. nicht anwendbar zu erklären. Eine entsprechende Bezeichnung kann lediglich als ein wiederlegbares Indiz betrachtet werden. Dabei spielt es keine Rolle, daß die Stellungnahme nach Lage der Akten erfolgen sollte. Zwar wird in der Regel ein Gutachten vorliegen, wenn zuvor eine körperliche Untersuchung stattgefunden hat. Bei einem Gutachten nach Lage der Akte wird lediglich keine erneute Befunderhebung vorgenommen. Das Gutachten wird dann auf die bereits vorliegenden Ergebnisse gestützt. Entscheidendes Merkmal für ein Gutachten ist die Bewertung durch einen medizinischen Sachverständigen. Die Würdigung der Befunde und Beschreibung von Unstimmigkeiten in einem bereits vorliegenden Gutachten unter Einsatz des Fachwissens eines medizinischen Sachverständigen erfüllt bereits die Voraussetzungen eines Gutachtens im Sinne des § 200 Abs. 2 SGB VII. Mit dieser Vorschrift beabsichtigt der Gesetzgeber die Stärkung der Rechte der Versicherten und eine Verbesserung der Transparenz im Unfallversicherungsverfahren. Damit hat er an die inhaltliche Entscheidungsgrundlage und nicht an formale Aspekte – wie Bestellung oder Abrechnung – angeknüpft.

Meine Auffassung entspricht auch dem Willen des Gesetzgebers. So heißt es im Bericht des federführenden Arbeits- und Sozialausschusses: *„Es bestand auch Übereinstimmung, daß sich die im Ausschuß neu beschlossene Regelung des Artikels 1 § 200 auch auf die Vergabe von Gutachten nach Aktenlage erstreckt“* (BT-Drs. 13/4853 vom 12. Juni 1996, S. 13).

Den Verstoß gegen §§ 200 Abs. 2 SGB VII, 76 Abs. 2 SGB X habe ich gem. §§ 81 Abs. 2 SGB X i.V.m. 25 Abs. 1 BDSG wegen der mangelnden Vorschläge zur Gutachterauswahl und des fehlenden Hinweises auf ein Widerspruchsrecht **beanstandet**.

Auch hier liegt es am Bundesversicherungsamt, sich der Sache weiter anzunehmen.

23.5 Kontrolle der Großhandels- und Lagerei-Berufsgenossenschaft

Anknüpfend an die Kontrolle im Jahre 1996 (vgl. 16. TB Nr. 23.4.4) habe ich den Gutachtereinsatz der Großhandels- und Lagerei-BG erneut kontrolliert.

Deren Gutachterdatei wird auf der Grundlage der Gutachterliste des Landesverbandes der gewerblichen Berufsgenossenschaften geführt und dient vorrangig dem Zweck, eine hinreichende Anzahl geeigneter Ärzte für Begutachtungen im Rahmen des unfallversicherungsrechtlichen Feststellungsverfahrens bereitzuhalten Diese Gutachterdatei ist ein erster wesentlicher Schritt hin zu mehr Transparenz im Zusammenhang mit dem Einsatz von Gutachtern.

Bei der Kontrolle der Gutachterdatei bin ich auf zwei Einzelfälle gestoßen, die besonders gut datenschutzrechtliche Probleme des Gutachtereinsatzes focussieren (vgl. auch Nr. 23.4).

– **Auswahl eines Gutachters**

Bei meiner Kontrolle im Jahre 1996 stellte ich Eintragungen zu zwei Gutachtern in der Datei fest, die von Sozialgerichten als befangen bewertet wurden. Die gespeicherten Daten wiesen Ungereimtheiten auf. Hierzu erklärte die BG, der HVBG hätte nur zu einem der Gutachter ein Urteil, in dem dieser als befangen zugunsten der Versicherten dargestellt wurde, an alle Berufsgenossenschaften versandt. Das hatte zur Folge, daß dieser Gutachter weder bei den Sozialgerichten noch von den Berufsgenossenschaften weiter eingesetzt wurde. Ich stellte der BG daraufhin eine Kopie eines Sozialgerichtsurteils zu dem anderen Gutachter zu, das ihm Befangenheit zugunsten der gesetzlichen Unfallversicherung vorwarf.

Meine Nachkontrolle im November 1997, mit der ich auch feststellen wollte, wie das – neue – SGB VII umgesetzt wird, ergab folgendes Bild:

Die Daten des einen als befangen zugunsten der Versicherten ausgewiesenen Gutachters waren aus der Datei gelöscht worden. Weiterhin gespeichert waren hingegen die Daten des anderen Gutachters. Wie ich weiter feststellen konnte, existiert zwischen diesem Gutachter und dem Landesverband Südwestdeutschland eine Sonderregelung, die dem Anschein nach auch auf die BG eine Bindungswirkung entfaltet. In dieser Sondervereinbarung wird dem Gutachter eine im Vergleich zum Ärzteabkommen besondere Gutachtenpauschale und eine von drei auf acht Wochen verlängerte Frist zur Erstellung des Gutachtens eingeräumt.

Die BG und das Bundesversicherungsamt habe ich um Stellungnahme gebeten, ob nicht auch die Daten des zweiten Gutachters aus der Gutachterdatei zu löschen seien.

– **Problematischer Gutachtereinsatz eines beratenden Arztes**

Sowohl ein Gutachten des zuständigen gewerbeärztlichen Dienstes als auch ein umfangreiches externes ärztliches Gutachten (weit über 40 Seiten) bejahten das Vorliegen einer Berufskrankheit bei einem Versicherten. Der danach gleichwohl eingeschaltete beratende Arzt der Berufsgenossenschaft wurde mit dem Hinweis *„Sollten Sie eine andere Auffassung vertreten, bitten wir um eine ausführliche Begründung.“* um eine Stellungnahme gebeten. Dieser beratende Arzt verneinte jedoch mit einem eine knappe Seite langen Schriftsatz das Vorliegen einer Berufskrankheit. Auf diese Stellungnahme wurde dann der ablehnende Bescheid gestützt.

In derartigen Fällen, in denen dem beratenden Arzt die komplette Akte übersandt wird und er nach dem ihm erteilten Auftrag faktisch die Rolle eines „Obergutachters“ innehat, vertrete ich im Gegensatz zu der BG die Auffassung, daß § 200 Abs. 2 SGB VII angewandt werden muß, da kein Grund ersichtlich ist, in diesen Fällen den beratenden Arzt anders als einen externen Gutachter zu behandeln (s. auch Nr. 23.4.2).

Darüber hinaus habe ich der BG die Frage gestellt, ob in derartigen Fällen mit dem Gutachter, dessen Gutachten nicht gefolgt wird, seitens der BG Kontakt aufgenommen wird, um evtl. Mißverständnisse zu klären und ihm Gelegenheit zu geben, sich mit der Auffassung des beratenden Arztes auseinanderzusetzen. Hierzu hat mir die BG mitgeteilt, daß in Fällen eines mißverständlich abgefaßten Gutachtens, in denen sie dem Gutachten nicht zu folgen beabsichtigt, Kontakt mit dem Gutachter aufgenommen werde. Diese Praxis begrüße ich sehr. Darüber hinaus halte ich es für überlegenswert, ob eine Rückkoppelung zum Gutachter in Fällen, in denen die BG seinem Votum nicht zu folgen beabsichtigt, angemessen und vernünftig ist, um dem Transparenzgebot zu genügen und evtl. nicht erforderliche Übermittlungen/Nutzungen oder Doppeluntersuchungen (vgl. § 62 SGB I) zu vermeiden.

23.6 Datenaustausch mit den Leistungserbringern

In der gesetzlichen Unfallversicherung ist beabsichtigt, den mit den Leistungserbringern anfallenden Schriftverkehr (z. B. ärztliche Gutachten) einschließlich der Abrechnungsunterlagen mittels kommerzieller Dienstleister auf elektronischem Wege an die Berufsgenossenschaften zu übermitteln. Bislang geschah das per Post.

In der Sache besteht zwischen dem BMA, dem HVBG und mir Einigkeit darin, das hohe Niveau der in anderen Zweigen der gesetzlichen Sozialversicherung zum automatisierten Datenaustausch entwickelten Lösungen auch auf die gesetzliche Unfallversicherung zu übertragen. An die Normenklarheit der Übermittlung legalisierender Vorschriften sind wegen des damit verbundenen Eingriffs in das Recht auf informationelle Selbstbestimmung des Versicherten und des Arztes sowie die dadurch bewirkte Durchbrechung des Arztgeheimnisses nach § 203 StGB besondere Anforderungen zu stellen. Ich verweise hierzu auf die beispielhaften Regelungen im SGB V und SGB XI.

Gesetzgeberischer Nachbesserungsbedarf besteht daher in den folgenden Punkten:

Die Vorschriften des SGB VII reflektieren nicht die besondere Qualität einer Verarbeitung auf Datenbändern oder maschinell verwertbaren Datenträgern (vgl. hingegen §§ 284 Abs. 1 Satz 2, 295 Abs. 5, 297 Abs. 4 SGB V sowie § 105 Abs. 1 Satz 2 SGB XI).

§ 199 SGB VII enthält weder eine ausdrückliche Befugnis zur Erhebung und Speicherung der Abrechnungsdaten (vgl. § 284 Abs. 1 Nr. 8 SGB V, § 94 Abs. 1 Nr. 5 SGB XI) noch eine besondere Befugnis der Leistungserbringer, Daten an Unfallversicherungsträger für Abrechnungszwecke zu übermitteln (vgl. §§ 294 ff. SGB V, § 104 Nr. 3 SGB XI). Zudem fehlt eine Vorschrift zur Einschaltung der mit der Datenverarbeitung beauftragten Stellen, wie sie in § 294 SGB V und § 104 SGB XI enthalten ist.

Darüber hinaus fällt auf, daß das SGB VII keine datenschutzrechlichen Regelungen zu Wirtschaftlichkeitsprüfungen oder Qualitätssicherungsmaßnahmen enthält. Sollten diese Verfahren in vergleichbarer Form so wie in der gesetzlichen Kranken- (§§ 296 ff, 135 SGB V) oder der gesetzlichen Pflegeversicherung (§§ 79f. SGB XI) auch in der gesetzlichen Unfallversicherung durchgeführt werden, müßten entsprechende Rechtsgrundlagen geschaffen werden.

23.7 Einzelfälle

23.7.1 Wer ist beteiligt?

Ein Petent hatte mit einem auch von anderen Landesverbänden verwendeten Formularvordruck eine Ermächtigung zur Durchführung arbeitsmedizinischer Vorsorgeuntersuchungen beantragt. In dem Antragsformular wurden umfangreiche Daten über seine ärztliche Qualifikation durch Ausbildung, Fortbildungsmaßnahmen, klinische Tätigkeiten und Publikationen sowie die sächliche und personelle Ausstattung von Labor- und Untersuchungsräumen erhoben. Im Schlußabsatz des Erhebungsbogens war eine Einwilligungsklausel aufgeführt. Damit erklärte sich der Unterzeichner einverstanden, daß seine Daten *„an die beteiligten Stellen“* wegen der beantragten Vorsorgeuntersuchungen weitergeleitet würden.

Die bei dem Landesverband Bayern und Sachsen der gewerblichen Berufsgenossenschaften (LVBG) beantragte Ermächtigung wurde dem Petenten vom Bayerischen Landesamt für Arbeitsschutz, Arbeitsmedizin und Sicherheitstechnik (LfAS) erteilt. Der Petent wandte sich dagegen, daß seine Daten ohne sein Wissen an eine ihm völlig unbekannte Stelle weitergegeben worden waren. Die Weitergabe der Daten an das LfAS aufgrund der Einwilligungserklärung in dem Formularvordruck halte ich für zu wenig bestimmt, da sich aus der Formulierung „an die beteiligten Stellen“ nicht ersehen läßt, an wen die Daten tatsächlich weitergegeben werden.

Der Handhabung liegt folgender Sachverhalt zugrunde: Die Zuständigkeit für die Erteilung einer Ermächtigung für die Vornahme spezieller arbeitsmedizinischer Vorsorgeuntersuchungen richtet sich danach, ob sich diese nach berufsgenossenschaftlichen oder nach staatlichen Vorschriften bestimmt. Im Bereich des LVBG hat sich ein unbürokratisches Ermächtigungsverfahren bewährt:

Anträge auf Ermächtigung zur Vornahme spezieller arbeitsmedizinischer Vorsorgeuntersuchungen in Verbindung mit den berufsgenossenschaftlichen Grundsätzen, sei es nach berufsgenossenschaftlichen und/oder staatlichen Vorschriften, können generell bei dem LVBG gestellt werden. Bei Zuständigkeit des LfAS wird der Antrag an dieses weitergeleitet.

Aus der insoweit nicht ausreichend konkreten Formulierung der Einwilligungserklärung ist dieses Verfahren aber nicht ersichtlich. Eine wirksame Einwilligung setzt voraus, daß der Zweck einer vorgesehenen Übermittlung erkennbar ist. Dafür ist auch eine Festlegung der Stellen erforderlich, die zur Verarbeitung und Nutzung von Daten berechtigt sein sollen. Nach dem Grundsatz der Transparenz der Datenerhebung, –nutzung und –verarbeitung soll der Betroffene jederzeit klar erkennen können, an welche Stellen seine Daten übermittelt werden.

Nachdem ich dem LVBG meine Bedenken mitgeteilt hatte, wurde die Einwilligungserklärung in den Ermächtigungsbögen in Abstimmung mit den übrigen Landesverbänden und dem HVBG in vorbildlicher Weise neu gestaltet. Die Erklärung ist nunmehr deutlich vom vorstehenden Text abgehoben und die Stellen, an die Unterlagen zur Prüfung der Ermächtigungsvoraussetzungen weitergeleitet werden, sind ausdrücklich benannt. Mit der Neufassung der Einwilligungserklärung ist eine deutliche Verbesserung der Transparenz im Ermächtigungsverfahren zur Durchführung arbeitsmedizinischer Vorsorgeuntersuchungen erreicht worden.

23.7.2 Anruf genügt . . . Sozialdetektive in der gesetzlichen Unfallversicherung

Immer wieder wird auch in den Medien über die Bekämpfung mißbräuchlicher Inanspruchnahme von Sozialleistungen berichtet, wobei Datenabgleiche oder der Einsatz von Außendienstmitarbeitern stets eine wichtige Rolle spielen. Ein Petent hat nun auf einen für mich neuen Aspekt der Bekämpfung von Leistungsmißbrauch aufmerksam gemacht, den Einsatz von Detekteien.

Der Petent erhielt nach einem schweren Arbeitsunfall von der Verwaltungs-Berufsgenossenschaft im Rahmen der Rehabilitation Pflegeleistungen. Nachdem es mehrfach zu Unstimmigkeiten über einzelne Abrechnungen (Inanspruchnahme von Pflegekräften und deren Anfahrtkosten) gekommen war, entstand bei der Verwaltungs-Berufsgenossenschaft der Verdacht, daß der Petent über einen längeren Zeitraum hinweg überhöhte Leistungen abgerechnet haben könnte. Sie beauftragte daher eine Detektei, an sieben aufeinanderfolgenden Tagen zu recherchieren, wann der Petent durch namentlich benannte Pflegekräfte betreut wurde und welche Fahrten die Pflegekräfte in diesem Zusammenhang durchgeführt hatten. Der Umfang der Datenerhebung wurde in dem Auftrag der Verwaltungs-Berufsgenossenschaft an die Detektei u. a. wie folgt formuliert:

„Sollten sich darüber hinaus bezüglich Art und Umfang der Pflege- bzw. Betreuungstätigkeit der vorgenannten Person oder zur tatsächlichen Pflegebedürftigkeit weitere Informationen ergeben, bitten wir, uns diese ggf. auch mitzuteilen.“

Die Detektei hat den ihr erteilten Auftrag – mit Ausnahme eines kurzen Gesprächs unmittelbar mit dem Petenten – in erster Linie durch verdeckt geführte Beobach-

tungen und verschiedene Beweisfotos sowie durch ein Gespräch mit einer dritten Personen erfüllt.

Die Beauftragung der Detektei zur Überprüfung der Abrechnungen des Petenten war aus datenschutzrechtlicher Sicht unverhältnismäßig und daher nicht zulässig:

Auch wenn die Einschaltung einer Detektei in Ausnahmefällen zulässig sein kann, so ist jedenfalls Voraussetzung, daß das gesetzlich vorgesehene Instrumentarium im Umgang mit evtl. Leistungsmißbrauchsfällen vorher ausgeschöpft wird. Die Verwaltungs-Berufsgenossenschaft hat sich mir gegenüber darauf berufen, daß die Beauftragung der Detektei notwendig gewesen sei, um ein Erstattungsverfahren nach § 50 SGB X durchzuführen. Diese Auffassung überzeugt mich nicht. Die Durchführung des Erstattungsverfahrens ist gem. § 60 Abs. 1 Satz 2 I.V.m. § 66 SGB I bereits dann möglich, wenn der Petent seinen Mitwirkungsobliegenheiten nicht nachkommt. Einer Observation bedurfte es nicht.

Zudem wurde durch den sehr weitgehend und unpräzise formulierten Ausforschungsauftrag der vertragliche Rahmen für eine nicht erforderliche Datenerhebung geschaffen. So enthält auch der Bericht der Detektei folgende Aussage:

„Dabei wird festgestellt, daß sich Frau X ebenfalls in der Wohnung aufhält. Sie trägt einen „Morgenmantel“. Während des Gesprächs geht Frau X keinen Tätigkeiten nach, die einen pflegerischen Charakter hätten. Herr Z bewegt sich in seiner Wohnung sehr behende und selbstständig. Aus dem Verhalten des Herrn Z, insbesondere seinen kurzen Wortwechseln mit Frau X wird deutlich, daß sich beide Personen „Duzen“ und in einem partnerschaftlichen Verhältnis zueinander stehen.“

Den Verstoß gegen die Erforderlichkeit der Datenerhebung gemäß § 67a Abs. 1 SGB X habe ich – wie auch die Verstöße wegen Datenerhebungen ohne Hinweis auf die Rechtsposition des Petenten nach § 67a Abs. 3 SGB X als auch der befragten dritten Person nach § 67a Abs. 4 SGB X – gemäß § 81 Abs. 2 SGB X i.V.m. § 25 Abs. 1 BDSG **beanstandet**.

23.7.3 Schweigen ist Gold

Nach einem Arbeitsunfall eines Petenten sollte im Rahmen eines gemeinsamen Gespräches zwischen ihm, seinem Arbeitgeber und dem Rehabilitations-Betreuer der Großhandels- und Lagerei-Berufsgenossenschaft geklärt werden, ob eine Wiedereingliederung bzw. Weiterbeschäftigung im Betrieb des Arbeitgebers möglich ist. Im Laufe des Gespräches schilderte der Petent ausführlich seine Krankheitsbilder und Beschwerden. Um klarzustellen, daß die unfallbedingten Beeinträchtigungen nicht das Ausmaß der dargelegten Beschwerden rechtfertigen könne, wies der Rehabilitations-Betreuer darauf hin, daß die unfallbedingte Erwerbsminderung 20% betrage.

Nachdem der Arbeitgeber unter Bezugnahme auf dieses Gespräch schriftlich um Auskunft bat, seit wann die Erwerbsminderung in Höhe von 20% bestehe, teilte die Berufsgenossenschaft dem Arbeitgeber das entsprechende Datum mit.

Da weder für die mündliche noch für die schriftliche Mitteilung der Berufsgenossenschaft an den Arbeitgeber des Petenten eine Rechtsgrundlage bestand, war die Datenübermittlung nicht zulässig. Von einer Beanstandung habe ich dennoch abgesehen. Einerseits hat die Berufsgenossenschaft die datenschutzrechtlichen Verstöße sofort eingeräumt und ihr Bedauern hierüber zum Ausdruck gebracht. Andererseits handelt es sich um einen durch besondere Umstände gekennzeichneten Einzelfall: In dem gemeinsamen Gespräch wurden von dem Petenten selbst medizinische Angaben gemacht, deren Auswirkungen auf seinen Arbeitseinsatz – wie beabsichtigt – diskutiert wurden. Es lag damit nahe, daß Informationen zu den Erkrankungen und deren Auswirkungen, wie auch zur Höhe der unfallbedingten Erwerbsminderung, ebenfalls zur Sprache kamen bzw. später – nach der mündlichen Offenbarung – schriftlich bestätigt und erläutert wurden.

So begrüßenswert grundsätzlich der Versuch ist, durch gemeinsame Gespräche zu einem für alle Beteiligten tragbaren Ergebnis zu gelangen, sind aus Datenschutzsicht derartige Gesprächssituationen zwischen Berufsgenossenschaft, Arbeitgeber und Versichertem nicht ohne Risiko. Sowohl im Verhältnis zwischen Berufsgenossenschaft und Arbeitgeber als auch zwischen Berufsgenossenschaft und Versichertem sowie zwischen Arbeitgeber und Versichertem gelten spezifische Erhebungs- und Übermittlungsvorschriften, die in der „Gemengelage“ eines Gesprächs kaum eindeutig abzugrenzen sind. Nach den derzeitigen Erfahrungen halte ich es jedoch für ausreichend, wenn die Gesprächspartner auf die jeweiligen datenschutzrechtlichen Rechtspositionen – etwa diejenige, daß der Arbeitgeber keine Diagnosen von der BG erfahren darf – hingewiesen werden.

Da diese Problematik durch die zunehmende Akzeptanz einvernehmlicher Lösungen künftig sicherlich an Bedeutung gewinnt, wird abzuwarten sein, ob darüber hinausgehende Hinweise oder Klarstellungen gegenüber den Berufsgenossenschaften erforderlich sein werden.

23.7.4 Gleich den Arbeitgeber fragen?

Mir ist aus verschiedenen Eingaben bekannt geworden, daß Berufsgenossenschaften zur Berechnung von Leistungen in noch laufenden Verfahren auf Anerkennung einer Berufskrankheit die Höhe des Arbeitsentgeldes sofort bei den Arbeitgebern erfragen, ohne den Petenten dies mitzuteilen oder diese um Zustimmung zu einer entsprechenden Anfrage bitten.

Von den Berufsgenossenschaften wird dazu die Auffassung vertreten, daß diese Erhebung ohne Mitwirkung des Betroffenen gem. § 67a Abs. 2 Satz 2 SGB X i.V.m. § 98 SGB X bzw. § 192 Abs. 3 SGB VII zulässig sei.

Mit dieser Praxis wird der Ersterhebungsgrundsatz, den ich bereits in meinem 15. TB (Nr. 10.2) als ein Querschnittsproblem der Sozialversicherung dargestellt habe, nahezu in sein Gegenteil verkehrt. Nach der Regelung des § 67a Abs. 2 Satz 1 SGB X sind Daten grundsätzlich beim Betroffenen bzw. unter seiner Mitwirkung gemäß § 60 Abs. 1 Nr. 1, zweite Alternative SGB I zu erheben. Der Vorrang der Datenerhebung unter Mitwirkung des

Betroffenen leitet sich aus dem informationellen Selbstbestimmungsrecht ab. Nur dann, wenn der Betroffene keine Angaben macht oder seine Zustimmung verweigert, können die zur Prüfung des Anspruchs erforderlichen Daten bei Dritten nach § 67a Abs. 2 Satz 2 SGB X erhoben oder die beantragte Leistung kann nach § 66 SGB I versagt werden.

Dieses datenschutzfreundliche Vorgehen hat in der Regel keinen bürokratischen Aufwand oder Zeitverzögerungen im Verfahren zur Folge, da die Bitte um Zustimmung mit dem obligatorischen Hinweis an den Versicherten nach § 67a Abs. 3 SGB X (u. a.: Folgen der Verweigerung von Angaben) verbunden werden kann.

24 Pflegeversicherung

24.1 Gemeinsame Verarbeitung und Nutzung personenbezogener Daten durch Kranken- und Pflegekassen

Da die Aufgaben von Kranken- und Pflegeversicherung eng miteinander verzahnt sind, legt § 96 SGB XI die Rahmenbedingungen fest, unter denen eine gemeinsame Verarbeitung und Nutzung personenbezogener Daten zulässig ist.

Die Umsetzung des § 96 SGB XI wirft jedoch einige Probleme auf:

- Die Daten, die gemeinsam verarbeitet und genutzt werden sollen, sind abschließend unter meiner Beteiligung und der des BMA festzulegen. Es erscheint nach wie vor im Hinblick auf die von den Kassen verwendeten unterschiedlichen Programme und Systeme fraglich, ob der bereits bestehende Datenkatalog weiter präzisiert werden kann (vgl. 16. TB Nr. 24.1).
- Abs. 2 der Vorschrift sieht u. a. vor, daß in den Fällen, in denen personenbezogene Daten von einem Arzt den Kranken- oder Pflegekassen zugänglich gemacht worden sind, die Übermittlungsbefugnis nach § 76 SGB X eingeschränkt ist. Es erscheint jedoch zweifelhaft, ob diese Regelung wortgetreu anzuwenden ist und damit bei einer Übermittlung etwa von einer Krankenkasse an eine Pflegekasse eine Einwilligung einzuholen ist. Dies hätte zur Folge, daß in den Fällen, in denen sich der Pflegezustand des Versicherten z. B. nach einer Krankenhausbehandlung verbessert, die Krankenkasse bei nicht erteilter Einwilligung gehindert ist, die Verbesserung der Gesundheitsverhältnisse der Pflegekasse mitzuteilen.
- Es kommt hinzu, daß nach meinen Erkenntnissen im allgemeinen Mitarbeiter der Kasse gleichzeitig sowohl Aufgaben der Kranken- als auch Pflegeversicherung wahrnehmen, so daß bereits allein aus diesem Grund eine klare Trennung der Datenbestände von Kranken- und Pflegkassen möglicherweise nicht durchführbar erscheint.

Da mir die Praxis der Kassen aufgrund der vielfältigen Verflechtungen dieser beiden Versicherungszweige aber sachgerecht erscheint und den Bedürfnissen der Versicherten, den organisatorischen Rahmenbedingungen aller Kassen sowie deren Beratungsauftrag nach § 7 Abs. 1 SGB XI entspricht, habe ich mich mit dem BMG, dem BMA und den Spitzenverbänden der gesetzlichen Krankenversicherung in Verbindung gesetzt, um Lösungen – ggf. gesetzgeberischer Art – zu den geschilderten Umsetzungsfragen zu erarbeiten.

24.2 Kontrollen von Pflegekassen

Im Berichtszeitraum habe ich zwei große Geschäftsstellen der BEK und der DAK kontrolliert. Dabei hat sich der Eindruck, den ich aus den wenigen Eingaben auf dem Gebiet der Pflegeversicherung insgesamt gewonnen habe, bestätigt:

Es handelt sich datenschutzrechtlich um einen gut bestellten Sozialversicherungszweig.

Ich mußte lediglich auf die Ergänzung der Dienstanweisungen in einem Sonderfall hinweisen:

Nach § 18 Abs. 4 Satz 1 SGB XI sind die Pflege- und Krankenkassen verpflichtet, dem Medizinischen Dienst die für die Begutachtung erforderlichen Unterlagen vorzulegen. Satz 2 dieser Vorschrift verweist auf § 276 Abs. 1 Sätze 2 und 3 SGB V, wonach eine Einwilligung für die Weitergabe von Unterlagen an den Medizinischen Dienst der Krankenversicherung vorgesehen ist, die der Versicherte über eine nach den §§ 60, 65 SGB I bestehende Mitwirkungspflicht hinaus der Pflegekasse überlassen hat.

Entsprechende Ergänzungen wurden mir zugesagt.

25 Gesundheit

25.1 Patient und Computer

Bekanntlich geht kaum etwas anderes jedem Menschen so nahe wie seine eigene Gesundheit. Und so sehr wir außer auf Hilfe, Zuwendung und Zuspruch auch auf neue Techniken hoffen, so sehr wollen wir gerade hier selbst darüber bestimmen können, wer was unter welchen Umständen über unsere Gesundheitsprobleme erfährt. Und gerade hier weckt der technische Fortschritt nicht nur Hoffnungen, sondern auch Angst:

Gentechnik, Klonen, die scheinbare Berechenbarkeit des Menschen durch seine Reduktion auf die Ergebnisse einer DNA-Analyse und dagegen sein Anspruch auf Eigenwert und auf die Anerkennung seiner nicht aus biologischen Erbfaktoren berechenbaren Würde, Computermedizin als Komparativ des bösen Wortes Apparatemedizin und die Furcht, daß irgendwann die Wirtschaftlichkeit – als Quotient aus dem gesellschaftlichen Nutzen einer Behandlung einerseits und den gegebenenfalls entstehenden Kosten andererseits – einmal über Leben und Tod entscheiden könnte, sind die Gründe dafür, daß beim Computereinsatz im Gesundheitswesen die Hoffnungen auf bessere Hilfe durch diese Technik und die Ängste vor dieser Technik enger beieinander liegen

als auf irgendeinem anderen Gebiet. Die Entscheidungen über die Gestaltung der Datenverarbeitung für Gesundheitszwecke werden deshalb das Bild in den Köpfen – aber fast noch stärker in den Herzen der Menschen – prägen, das sie sich von der zukünftigen Informationsgesellschaft machen.

Es gibt also viele Gründe, den Schutz der Gesundheitsdaten auch und gerade unter den Bedingungen der modernen Datenverarbeitung solide und für jedermann glaubwürdig zu gewährleisten, d. h., die ärztliche Schweigepflicht auch in der Zukunft ernstzunehmen. Nach meinen Erfahrungen ist das denjenigen, die für das Gesundheitswesen Verantwortung tragen, auch durchweg bewußt.

25.2 Netze für Patientendaten

In der Medizin wird auf vielen Teilgebieten zunehmend moderne Informationstechnik eingesetzt, und zwar nicht nur in neuen Untersuchungsverfahren wie Computer-Tomographie, sondern z. B. auch in der Labordiagnostik und in Röntgengeräten, die primär statt Bildern Daten liefern, aus denen in einem zweiten Schritt zur Befundung geeignete Bilder erzeugt werden. Daneben führt der PC-Einsatz in der ärztlichen Praxis dazu, daß bislang schriftlich geführte Unterlagen digitalisiert gespeichert sind. Nachdem zugleich die Leistungsfähigkeit der Datenfernübertragung bei eher sinkenden Preisen stark zugenommen hat, liegt es nahe, für die Behandlung von Patienten auch Netze zur Übertragung digitaler Daten zu nutzen. Weil die Entwickler wie die Anwender solcher Systeme von vornherein Datenschutz und ärztliche Schweigepflicht berücksichtigen wollten, waren Datenschutzbeauftragte aus Bund und Ländern an vielen Überlegungen und Entwicklungen dazu beteiligt.

25.2.1 Telekonsultation

Die Datenübertragungsmöglichkeiten erleichtern es dem behandelnden Arzt, einen Kollegen zur Beratung heranzuziehen, weil viele relevante Informationen auf einfache und kostengünstige Weise schnell übertragen werden können. An der Zulässigkeit der Übermittlung der Patientendaten an den Kollegen ändert sich dadurch nichts. Bei der Nutzung der Datenübertragungstechnik ist aber zu berücksichtigen, daß die Angaben unterwegs verfälscht oder auch unbefugt zur Kenntnis genommen werden könnten, und der behandelnde Arzt muß sich davon überzeugen, daß er die Daten tatsächlich dem gewünschten Kommunikationspartner schickt. Wenn – wie heute üblich – als technische Basis aus Kosten- und Leistungsgründen das Internet gewählt wird, sind dafür besondere Maßnahmen zu treffen.

Die Authentizität von Kommunikationspartnern in medizinischen Netzen kann durch den Einsatz von Health-Professional Cards (HPC) gewährleistet werden. Der ist in der Regel auch von den Entwicklern eingeplant, HPC sind aber noch nicht allgemein eingeführt (s. o. Nr. 9.1.1). Bis das erfolgt ist, müssen statt dessen andere Mittel genutzt werden, z. B. für das jeweilige medizinische Netz und seine Benutzer eingerichtete Authentifizierungsserver, die im Prinzip dasselbe leisten können, aber die Interoperabilität verschiedener Netze stören.

Das Verfälschen, das unbefugte Mitlesen und sogar das unbefugte Speichern von Daten auf ihrem Weg durch ein modernes Kommunikationsnetz lassen sich nicht ausschließen, Sicherungsmaßnahmen können jedoch verhindern, daß dadurch relevante Schäden entstehen.

- Das **Verfälschen** von Daten läßt sich zuverlässig erkennen, wenn der Empfänger die vom Absender hinzugefügte digitale Signatur prüft. Das geschieht schnell und automatisch, und wenn diese Verfahren eingeführt sind – wobei ebenfalls der HPC eine Schlüsselrolle zugedacht ist – wird der einzige Schaden einer Verfälschung darin liegen, daß die Datenübertragung zu wiederholen ist.
- Der Schaden, der **durch unbefugtes Mitlesen oder Speichern** von im Netz übertragenen Patientendaten entstehen könnte, läßt sich durch sichere kryptographische Verschlüsselung der zu übermittelnden Angaben vermeiden. Die Verfahren und die verwendeten Schlüssellängen müssen jedoch so gewählt sein, daß sie auch nach Jahrzehnten den dann noch immer gebotenen Schutz gewährleisten. Denn es wäre fatal, wenn schutzbedürftige Angaben, die heute über ein Netz verschickt werden, als zunächst nicht entschlüsselbar unbefugt aufgezeichnet und dann 20–30 Jahre später entschlüsselt und bekanntgemacht würden. 20–30 Jahre sind für die Entwicklung der Informationstechnik zwar viel Zeit, aber ein heute Zwanzigjähriger ist danach erst etwa 45 Jahre alt, und damit bestimmt noch an der Geheimhaltung seiner Gesundheitsdaten interessiert.

Die für Datenübertragungen im Rahmen von Telekonsultationen gebotenen Maßnahmen sind auch zu treffen, wenn **Arztbriefe** und ähnliche Mitteilungen zur Betreuung eines Patienten über ein Netz versandt werden.

25.2.2 Die virtuelle elektronische Patientenakte

Ein auf der Basis bekannter – wenn auch noch nicht immer voll verfügbarer – Technik erreichbares Fernziel der Vernetzung ist die virtuelle elektronische Patientenakte: Die an unterschiedlichen Stellen vorliegenden Angaben eines Patienten sollen so über ein Kommunikationsnetz zugreifbar sein, daß bei Bedarf die zu seiner weiteren Behandlung oder Betreuung hilfreichen Angaben leicht genutzt werden können. Zwar sind noch längst nicht alle relevanten Angaben so digitalisiert, daß sie ohne weitere Vorarbeiten in einem Netz übertragbar wären. Mit dem zunehmenden Einsatz moderner Informationstechnik für die medizinische Dokumentation wird dieses Problem aber geringer, und die Sicherheit bei der Übertragung kann mit den Mitteln gewährleistet werden, die Datenübertragungen für Zwecke der Telekonsultation schützen (s. o. Nr. 25.2.1).

Anders als bei der Telekonsultation sind aber besondere Vorkehrungen zu treffen, um unzulässige Übermittlungen von Patientendaten zu verhindern. Denn wenn Angaben über die Gesundheit eines Patienten abgefragt werden, dann muß der Fragende nicht nur im Prinzip be-

rechtigt sein, Daten dieser Art zu erhalten – was er mit seiner HPC nachweisen könnte –, sondern auch die konkrete Anfrage muß zulässig sein. Das heißt, die Weitergabe der Daten muß z. B. der weiteren Behandlung dienen, und außerdem muß der betroffene Patient mit der Datenweitergabe einverstanden sein.

Ob bei einer Anfrage tatsächlich Umstände vorliegen, die eine Übermittlung von Patientendaten in dem konkreten Einzelfall rechtfertigen, läßt sich mitunter von der ersuchten Stelle schlecht prüfen. Besonders kritisch wird diese Frage, wenn im automatisierten Verfahren darüber entschieden werden soll, ob die Antwort erteilt wird. Dabei bestehende Risiken könnten durch eine Protokollierung der Abfragen und eine wenigstens stichprobenweise nachträgliche Zulässigkeitskontrolle kompensiert werden. Lösungen, die so viel Sicherheit gegen unbefugte Nutzungen bieten, daß ein Arzt die ihm anvertrauten Gesundheitsdaten für zukünftige Online-Abrufe zur Verfügung stellen könnte, liegen derzeit noch nicht vor. Das Einverständnis der Patienten auch dazu zu verlangen, daß ihre Daten wegen des Fehlens angemessener Sicherungsmaßnahmen auch einmal mißbraucht werden könnten, halte ich aber für nicht hinnehmbar.

Ebenso ungelöst ist die Frage, wie zu einer – berechtigten – Anfrage die Stelle zu finden ist, von der die Antwort kommen kann. Eine Lenkungsmöglichkeit wäre ein zentrales Nachweissystem über Gesundheitsdaten, das zu Recht auf Bedenken stößt und zumindest weitere erhebliche Sicherungsprobleme aufwirft.

Insgesamt ist es nach meinen Erfahrungen und meinem Wissen immer noch so, daß die volle Nutzung moderner Informationstechnik für den Umgang mit Gesundheitsdaten nach wie vor viel Entwicklungsarbeit erfordert, wenn man nicht den Patienten die Risiken des Mißbrauchs ihrer Daten zumuten möchte. Eine vielfach wirksame Unterstützung denkbarer Lösungen dürften die auch in Netzen einsetzbaren HPC bieten, deren Einführung deshalb dringend gefördert werden sollte.

25.3 Professionalisierung der medizinischen Datenverarbeitung

Sowohl in den Projekten zur Nutzung von Chipkarten für das Gesundheitswesen als auch bei der Entwicklung von Netzen für Patientendaten sind oft engagierte Ärzte die treibende Kraft. Schon heute ist jedoch abzusehen, daß die intensive Nutzung der modernen Informationstechnik im Gesundheitswesen zu einer Arbeitsteilung zwischen behandelnden Ärzten und Datenverarbeitungs-Dienstleistern führt. Typische, nicht von Ärzten geleistete Dienste werden z. B. die Langzeitdokumentation von Patientendaten insbesondere für Krankenhäuser, die Wartung und Reparatur von Datenverarbeitungsanlagen sowie das Betreiben von Netzen und Nachweissystemen für Patientendaten sein.

Es wird sich nicht immer vermeiden lassen, daß die auf diesen Gebieten tätigen Gehilfen neuer Art, die nicht durch § 203 StGB zum Schutz von Privatgeheimnissen besonders verpflichtet sind, Gesundheitsdaten von Patienten zur Kenntnis nehmen oder zumindest die technische Möglichkeit haben, über diese Daten zu verfügen. Und ein Arzt, der solche Dienstleistungen in Anspruch nimmt, wird nicht unbedingt selbst über das Spezialwissen verfügen, um abschätzen zu können, welche Möglichkeiten der Dienstleister tatsächlich hat, in dessen Obhut er die ihm anvertrauten Patientendaten gibt.

Um die sinnvolle Nutzung moderner Informations- und Kommunikationstechniken im Gesundheitswesen zu fördern, sollte deshalb Klarheit über die Bedingungen geschaffen werden, unter denen ein Arzt seiner Schweigepflicht unterliegende Angaben einem Datenverarbeitungs-Dienstleister anvertrauen darf. Zu erwägen ist dabei auch, ob die (ärztliche) Schweigepflicht und die damit korrespondierenden Beschlagnahmeverbote und Aussageverweigerungsrechte auch auf bestimmte Verarbeitungen von Gesundheitsdaten durch Dienstleistungsunternehmen auszudehnen sind. Wegen der Geschwindigkeit, mit der sich der Einsatz moderner Informationstechnik im Gesundheitswesen entwickelt, sind alle Betroffenen aufgerufen, intensive Gespräche darüber zu führen, wie die in Rede stehenden Vorschriften im StGB und in der StPO zu erweitern und anzupassen sind.

25.4 Transplantationsgesetz

Die gute Zusammenarbeit mit dem BMG (s. 16. TB Nr. 25.2) und die intensiven und stets lösungsorientierten Diskussionen mit interessierten Ärzten haben dazu geführt, daß sachgerechte Vorschriften für den Umgang mit den personenbezogenen Daten von Spendern und Empfängern entworfen und schließlich als Teil des Transplantationsgesetzes (TPG) verabschiedet wurden.

Inzwischen hat das BMG mit Zustimmung des Bundesrates in einer allgemeinen Verwaltungsvorschrift das **Muster des Organspendeausweises** festgelegt. Entsprechend den Vorgaben in § 2 Abs. 2 TPG kann darin erklärt werden, ob man

– zur Transplantation die **Entnahme** von Organen und Gewebe aus seinem Körper nach der ärztlichen Feststellung des Todes **gestattet**,
– dies nur **mit Ausnahme** selbst benannter Organe/Gewebe **gestattet** (z. B. kein Auge),
– dies **nur für selbst benannte Organe/Gewebe gestattet** (z. B. Herz, Niere, Leber),
– der **Entnahme** von Organen und Gewebe zur Transplantation **widerspricht** oder
– **die Entscheidung** auf eine mit Namen, Telefon und Anschrift eingetragene Person übertragen hat.

Um die Vorstellungen der Betroffenen möglichst weitgehend zur Geltung zu bringen, kann die Erklärung durch Anmerkungen und besondere Hinweise individuell ergänzt werden.

Das BMG prüft, ob zusätzlich zu dem Angebot, die persönliche Entscheidung im Organspendeausweis zu dokumentieren, ein Organspenderegister eingerichtet werden soll. Sachgerechte Datenschutzvorgaben dazu sind in § 2 Abs. 3 und 4 TPG enthalten.

Die Vertragsverhandlungen über die nach §§ 11 und 12 TPG abzuschließenden Verträge über die Zusammenarbeit der Krankenhäuser mit der Koordinierungsstelle, bei der Organentnahme sowie über die Organ-Vermittlungsstelle werden voraussichtlich Mitte 1999 abgeschlossen. Probleme bei der Erfüllung der gesetzlichen Vorgaben zum Datenschutz für Spender und Empfänger haben sich dabei erfreulicherweise nicht ergeben.

25.5 Transfusionsgesetz

Die Erkenntnis, daß durch Bluttransfusionen und durch aus Blut gewonnene Produkte HIV und andere Krankheitserreger auf die Empfänger übertragen wurden, was zumindest zum Teil durch mehr Sorgfalt bei der Entnahme von Blutspenden hätte vermieden werden können, belegt eindrucksvoll die Notwendigkeit, den Gesundheitszustand von Blutspendern vor der Spende und das gespendete Blut sorgfältig zu prüfen. Um zu gewährleisten, daß diese auch Kosten verursachenden Maßnahmen regelmäßig durchgeführt werden, müssen ihre Ergebnisse für behördliche Kontrollen nachprüfbar dokumentiert werden.

Zusätzlich sind lückenlose Aufzeichnungen darüber geboten, wie eine Blutspende verwendet wurde und welche Patienten dieses Blut oder ein Produkt erhalten haben, in dem Bestandteile dieses Blutes enthalten sind. Denn wenn der begründete Verdacht aufkommt, daß ein Patient dadurch infiziert wurde, muß nicht nur feststellbar sein, von welchem Spender die Krankheitserreger stammen könnten, sondern es müssen alle Spenden dieses Spenders so lange von jeder weiteren Verwendung ausgeschlossen werden, bis deren Unbedenklichkeit feststeht. Aus diesen Gründen enthält das Transfusionsgesetz (TFG), das seit Mitte 1998 die Gewinnung von Blut und dessen Verwendung neu regelt, detaillierte Vorschriften über die Erhebung, Verarbeitung und Nutzung personenbezogener Daten sowohl der Spender als auch der mit Blut oder Blutprodukten behandelten Patienten.

In der intensiven konstruktiven Diskussion mit dem BMG und dem BMJ wurden dafür Lösungen erarbeitet, die alle Aspekte des Infektionsschutzes bei der Anwendung von Blut und Blutprodukten berücksichtigen und zugleich den Datenschutz der Blutspender und der Patienten gewährleisten. So begrenzt das TFG die Verarbeitung und Nutzung der personenbezogenen Daten auf die Zwecke der ärztlichen Behandlung, der Risikoerfassung nach dem Arzneimittelgesetz, der Sicherungszwecke nach dem Transfusionsgesetz und der Verfolgung solcher Straftaten und Ordnungswidrigkeiten, die im engen Zusammenhang mit der Spendenentnahme stehen. Außerdem ist jeder Blutspender nicht nur über die Umstände der Spendenentnahme, sondern auch darüber aufzuklären, welche Verarbeitungen seiner Daten notwendigerweise mit seiner Blutspende verbunden sind. Damit erfüllt das Transfusionsgesetz die Vorgaben der europäischen Datenschutzrichtlinie, die nicht nur besondere Vorkehrungen für den Schutz von Gesundheitsdaten, sondern auch eine umfassende Unterrichtung der Betroffenen über den Umgang mit ihren Daten verlangt (s. auch Nr. 2.1.).

26 Verteidigung

26.1 Behördliche Datenschutzbeauftragte innerhalb der Teilstreitkräfte der Bundeswehr

Mit dem BMVg habe ich diskutiert, ob innerhalb der Teilstreitkräfte die Aufgaben des behördlichen Datenschutzbeauftragten an der richtigen Stelle angebunden sind. Aufgabe des behördlichen Datenschutzbeauftragten sollte es sein, in seinem Zuständigkeitsbereich für eine ordnungsgemäße Verarbeitung personenbezogener Daten zu sorgen und dieses vor Ort etwa durch Einsicht in Personalakten zu kontrollieren. Ebenso sollte er ein „erster Ansprechpartner für den Datenschutz" – auch und gerade bei der Verarbeitung von Personaldaten – für alle Soldaten (Grundwehrdienstleistende, Zeit- und Berufssoldaten sowie Reservisten) sein, damit sie sich nicht sogleich an den für Personalangelegenheiten zuständigen Fachoffizier wenden müssen.

Dies ist bei der derzeitigen Organisation in den Teilstreitkräften der Bundeswehr nicht gewährleistet. Hiernach ist in der Regel der für das Führungsgebiet 1 (Personalwesen, Innere Führung, Presse-/Öffentlichkeitsarbeit) zuständige Offizier/Unteroffizier für den Datenschutz zuständig. Interessenkonflikte sind hier vorprogrammiert: Wenn auch der Personaloffizier in der Regel keine Personalentscheidungen trifft, ist er jedoch fachlich gehalten, Personaldaten zu erheben und für Entscheidungen zu speichern. Im Zweifelsfall müßte er sich insoweit selbst kontrollieren.

Das BMVg macht gegenüber meiner Kritik geltend, die Durchführung des BDSG und der anderen Vorschriften über den Datenschutz sei in seinem Geschäftsbereich sog. Linienaufgabe; (unabhängige) Datenschutzbeauftragte würden daneben nicht bestellt (siehe hierzu Durchführungsbestimmungen zum BDSG VBMl. 1998 S. 153, 162). Der zuständige Fachoffizier/-unteroffizier sei weder für Beschwerden von Soldaten, noch für datenschutzrechtliche Kontrollen zuständig. Dies solle auch in Zukunft so bleiben.

Wenn ich auch Probleme bei der Änderung des gegenwärtigen Zustands nicht verkenne, führe ich mit dem BMVg das Gespräch fort, um eine datenschutzrechtlich bessere Organisation des Datenschutzes durch die Bestellung des geeigneten Offiziers/Unteroffiziers zum internen Datenschutzbeauftragten zu erreichen.

26.2 Beratung und Kontrolle der Teilstreitkräfte der Bundeswehr

Bereits in meinem 16. TB (Nr. 26.1) hatte ich erfreulicherweise feststellen können, daß bei der Bundeswehr auch dem Datenschutz die gebotene Berücksichtigung zuteil wird. Diese Feststellung hat sich bei den weiteren Kontrollen und Beratungen eines Transportbataillons des Heeres und eines Geschwaders der Luftwaffe bestätigt. Ich habe nur wenige Mängel beim Umgang mit personenbezogenen Daten von Soldaten feststellen müssen. Ein Teil der Mängel basiert auf der Anwendung eines Erlasses des BMVg über die Führung der Personalun-

terlagen der Soldaten aus dem Jahre 1965, der durch das BMVg derzeit jedoch überarbeitet wird.

Im Berichtszeitraum hat das BMVg die für den gesamten Geschäftsbereich geltenden Durchführungsbestimmungen zum BDSG überarbeitet und neu bekanntgemacht (VMBl. 1998 S. 153). Ebenso ist positiv festzuhalten, daß in Teilstreitkräften der Bundeswehr bei der Fortbildung der für die Aufgabe Datenschutz zuständigen Offiziere im Rahmen der Laufbahn- und Verwendungslehrgänge das Thema Datenschutz in die Lehrpläne aufgenommen wurde. Dabei verkenne ich allerdings nicht, daß hier noch das eine oder andere mehr getan werden könnte.

26.3 Einsichtnahme der Musterungsärzte in Unterlagen der Kriegsdienstverweigerer

In meinem 16. TB (Nr. 26.3) habe ich über das mit dem BMVg erzielte Einvernehmen über den Umfang der Unterlagen berichtet, die den in den Kreiswehrersatzämtern tätigen Musterungsärzten zuzuleiten sind. Danach soll der Musterungsarzt im Interesse des Wehrpflichtigen Zugang zu dessen vollständiger Personalakte haben. Das BMVg setzte dieses Ergebnis in den einschlägigen Vorschriften um. Die neuen Verfahrensregelungen sahen allerdings auch vor, daß die Musterungsärzte Einsicht in die Unterlagen der Kriegsdienstverweigerer (Antrag und Begründung) nehmen dürfen, sofern sie dies für das Musterungsergebnis für erforderlich hielten; bisher waren diese Unterlagen während der gesamten Dauer der Musterung in einem verschlossen Umschlag aufzubewahren.

Hierzu habe ich das BMVg um Rücknahme der aus meiner Sicht zu weit gehenden Zulassung der Einsichtnahme gebeten. In meiner Begründung habe ich darauf hingewiesen, daß es sich bei der Einsichtnahme in die KDV-Unterlagen durch die Musterungsärzte um eine unzulässige Zweckänderung handelt, da die darin enthaltenen Daten ausschließlich für das KDV-Verfahren erhoben werden, das nach der Musterung vom Bundesamt für den Zivildienst durchgeführt wird. Im Hinblick auf die Argumentation des BMVg, diese Daten seien für die Entscheidung der Musterungsärzte erforderlich, habe ich darauf hingewiesen, daß die einschlägigen Vorschriften für die Musterungsärzte bereits vorsehen, daß ein Facharzt hinzugezogen werden kann, sofern aus ärztlicher Sicht weitergehende Untersuchungen erforderlich sind.

Das BMVg teilt grundsätzlich meine datenschutzrechtlichen Bedenken, unterstreicht aber die Notwendigkeit, dem Musterungsarzt im Einzelfall – bei konkreter Veranlassung – aus ärztlicher und insbesondere wehrmedizinischer Sicht eine Einsichtnahme in KDV-Unterlagen zu ermöglichen.

Im Interesse der Wehrpflichtigen an einem zuverlässigen Musterungsergebnis kann ich mich dieser Argumentation nicht verschließen. Ich habe mit dem BMVg Einvernehmen dahingehend erzielt, daß die Einsichtnahme in die verschlossenen KDV-Unterlagen des Wehrpflichtigen durch Musterungsärzte auch künftig grundsätzlich unzulässig ist, aber im medizinisch begründeten Einzelfall **mit schriftlicher Zustimmung des Wehrpflichtigen** erlaubt sein soll.

27 Zivildienst

– IT-Anschluß von Verwaltungsstellen ohne ausreichende Sicherungsmaßnahmen –

Bei der Kontrolle von Dienststellen für Zivildienstleistende konnte ich feststellen, daß einige nicht nur mit moderner Informationstechnik ausgestattet sind, sondern auch Zugänge zu Diensten des Internet (E-Mail, WWW) nutzen (zum Internet s. insbesondere Nrn. 8.3., 9.7 und 9.9).

Hiergegen habe ich zwar keine grundsätzlichen Bedenken. Jedoch dürfen auf den PC keine personenbezogenen Daten von Zivildienstleistenden verarbeitet werden, solange kein ausreichendes Sicherheitskonzept für an das Internet angeschlossene PC vorliegt. Dies bedeutet, daß die damit verbundenen möglichen Risiken analysiert und bewertet werden müssen, um die notwendigen technischen und organisatorischen Maßnahmen zum Schutz der Daten vorzusehen. Dies konnte bei keiner der kontrollierten Dienststellen im Bereich des BAZ festgestellt werden. Daraufhin habe ich dem BAZ empfohlen, bei diesen Dienststellen darauf zu dringen, PC mit Zugang zu Internet-Diensten isoliert von denjenigen PC zu betreiben, auf denen personenbezogene Daten von Zivildienstleistenden verarbeitet werden. Ich halte zur Zeit es für nicht verantwortbar, ohne zusätzliche Sicherungen PC an Internet-Dienste anzuschließen, auf denen personenbezogene von Zivildienstleistenden Daten verarbeitet werden.

28 Verkehrswesen

28.1 Neue straßenverkehrsrechtliche Regelungen

Der in meinem 16. TB unter Nr. 28.3 beschriebene Gesetzentwurf zur **Änderung des Straßenverkehrsgesetzes und anderer Gesetze** wurde inzwischen beschlossen und am 30. April 1998 verkündet (BGBl I S. 747). Er ist mit seinen wesentlichen Regelungen am 1. Januar 1999 in Kraft getreten. Damit wurden u. a. folgende aus datenschutzrechtlicher Sicht bedeutende Gesetzesänderungen geschaffen:

- Ausweitung der Online-Abrufe auf sämtliche beim KBA geführte Register mit angemessenen Vorkehrungen zum Datenschutz,
- Einrichtung eines neuen automatisierten Anfrage- und Auskunftsverfahrens unter den Bedingungen der neuesten Technik, das unabhängig vom Online-Betrieb sowohl Massen- als auch Einzelanfragen ermöglicht und im Ergebnis die gleiche Sicherheit wie bei Online-Abrufen gewährleistet,
- Entgeltfreiheit für Selbstauskünfte entsprechend den Regelungen des BDSG, wie es auch für andere Dateien der öffentlichen Verwaltung die Regel ist,
- Verlängerung der Aufbewahrungsfrist und eine akzeptable Erweiterung der zweckfremden Nutzung von Protokolldaten sowie

– Löschungsregelungen für die im Zusammenhang mit der Erteilung von Fahrerlaubnissen oder den Eignungsprüfungen erhobenen personenbezogenen Daten.

Ab 1. Januar 1999 wird neben den örtlichen Fahrerlaubnisregistern auch ein **Zentrales Fahrerlaubnisregister** beim KBA geführt. Örtliche Fahrerlaubnisregister dürfen, sofern die in § 65 Abs. 10 StVG genannten Voraussetzungen erfüllt sind, nur noch bis zum 31. Dezember 2005 geführt werden. Eine kürzere Übergangsfrist wäre wegen der Vermeidung unnötiger Doppelspeicherungen aus meiner Sicht zwar wünschenswert gewesen, der für den Schlußtermin gefundene Kompromiß ist aber vertretbar. Die detaillierten rechtlichen Regelungen (Verordnung, Verwaltungsvorschrift) sowie die technischen Bedingungen (Festlegung der Übermittlungsstandards) für die Kommunikation zwischen den örtlichen Fahrerlaubnisbehörden und dem KBA präzisieren die gesetzlichen Vorgaben zum Datenschutz und zur Datensicherung. Eine schematische Übersicht über die Nutzung der zentralen Register über Fahrzeuge und Fahrerlaubnisse geben die Abbildungen **16** und **17**.

Das Gesetz ergänzt auch das **Fahrlehrergesetz** und das **Kraftfahrsachverständigengesetz** um Regelungen zur Verarbeitung der Daten von Fahrlehrern, Fahrschulen und Fahrlehrerausbildungsstätten sowie von Sachverständigen und Prüfern für den Kraftfahrzeugverkehr. Dabei wurde der Datenschutz angemessen berücksichtigt.

28.1.1 Fahrerlaubnis-Verordnung

Die für die Umsetzung der fahrerlaubnisrechtlichen Regelungen des StVG erforderliche **Fahrerlaubnis-Verordnung – FeV –** wurde inzwischen mit der Verordnung über die Zulassung von Personen zum Straßenverkehr und zur Änderung straßenverkehrsrechtlicher Vorschriften vom 18. August 1998 (BGBl. I S. 2214) erlassen. An den mit meiner Beteiligung entstandenen datenschutzrechtlichen Regelungen des Regierungsentwurfs wurden aufgrund von Anträgen einiger Landesregierungen durch Beschluß des Bundesrates vom 19. Juni 1998 Änderungen vorgenommen, die aus meiner Sicht bedenklich sind und zum Teil im Widerspruch zu Wortlaut und Sinn des vom Deutschen Bundestag verabschiedeten StVG stehen. Deshalb halte ich es für geboten, alsbald einige Regelungen der Verordnung zu ändern:

– Das **Recht des Betroffenen auf Einsichtnahme in die** an eine Untersuchungsstelle oder an einen Gutachter zu übersendenden **Fahrerlaubnisunterlagen** sollte in § 11 Abs. 6 FeV ausdrücklich festgelegt werden. Damit könnten auch Zweifel ausgeräumt werden, ob und in welchem Umfang sich dieses Recht bereits aus dem Verwaltungsverfahrensgesetz ableiten läßt.

– § 2 Abs. 14 Satz 1 StVG schreibt vor, daß die Fahrerlaubnisbehörden den Stellen oder Personen, die die Eignung oder Befähigung zur Teilnahme am Straßenverkehr beurteilen oder prüfen**, nur die Daten übermitteln** dürfen, ***„die diese zur Erfüllung ihrer Aufgaben benötigen“***. Der Gesetzgeber weist damit die Aufgabe zur Trennung der Fahrerlaubnisakte ausdrücklich der übermittelnden Stelle zu. Dieses ist auch sinnvoll, da die Fahrerlaubnisbehörde als Herrin des Verfahrens entscheidet, welche Zweifel an der Eignung oder Befähigung auszuräumen sind, und daher auch beurteilen kann, welche **Unterlagen** für die Ausräumung dieser Zweifel **erforderlich** sind. Im übrigen hat die Fahrerlaubnisbehörde wegen der Beachtung der gesetzlichen **Verwertungsverbote** ohnehin zu prüfen, ob die Datenübermittlung zulässig ist. Dabei kann sie auch problemlos mit feststellen, welche Daten hierfür erforderlich sind. Statt dessen sieht § 11 Abs. 6 Satz 4 der Verordnung vor, daß die Fahrerlaubnisbehörde der untersuchenden Stelle die ***„vollständigen Unterlagen“*** übersendet. Damit würde die Aufgabe der Trennung der Unterlagen und die Beachtung der Verwertungsverbote auf eine mit dem Verwaltungsverfahren nicht vertraute Stelle verlagert, was insgesamt zu Mehraufwand und nicht selten zu Fehleinschätzungen und -bewertungen führen dürfte. Eine entsprechende Änderung der Verordnung ist unbedingt erforderlich, um den Auftrag des Gesetzgebers zu erfüllen.

– Die Regelung, daß sämtliche für den **Abruf im automatisierten Verfahren** bereitgehaltenen Daten aus dem Verkehrszentralregister (VZR) auch *„für alle sonstigen Stellen im Sinne des § 30 Abs. 1 und 3 des Straßenverkehrsgesetzes“* bereitgehalten werden sollen (§ 61 Abs. 4 a), steht im Widerspruch zu dem vom Gesetzgeber in § 30 Abs. 1 StVG erteilten Auftrag zur Beschränkung der zu übermittelnden Daten an die für bestimmte Aufgaben zuständigen Stellen. Hier ist eine präzisere Regelung in der Verordnung geboten, die dem tatsächlichen Informationsbedarf der jeweiligen Stellen entspricht.

– § 69 Abs. 3 ist dahingehend zu ändern, daß die für die Durchführung der **Fahrerlaubnisprüfung** erhobenen personenbezogenen Daten bereits nach Ablauf des auf die Erledigung des Prüfauftrages folgenden zweiten Kalenderjahres zu löschen sind, da die Verlängerung der **Löschungsfrist** auf fünf Jahre nur mit einem gesetzlich nicht vorgesehenen Zweck (Überwachung und zur Aufdeckung von Manipulationen) begründet wurde und daher nicht gerechtfertigt ist.

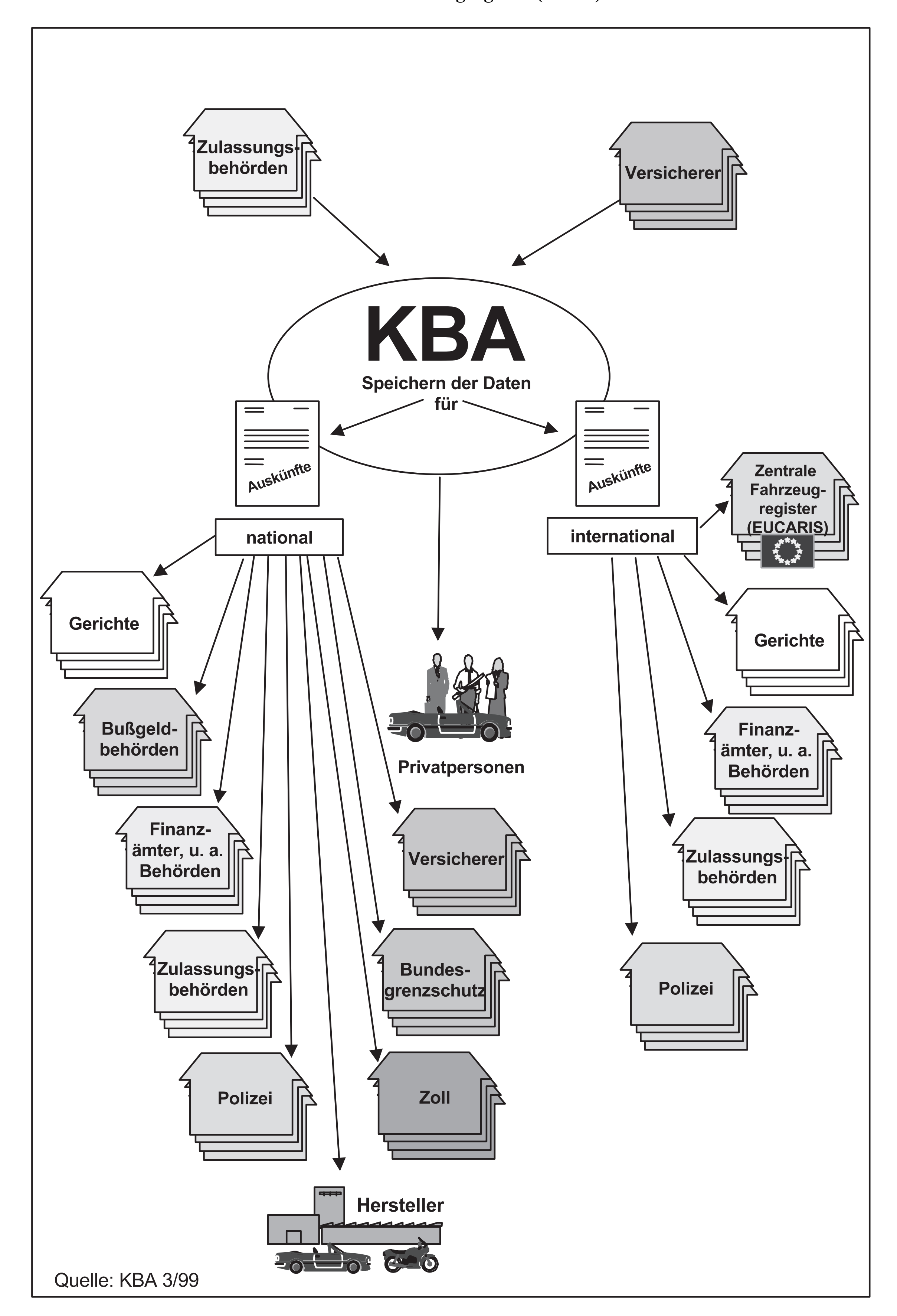
Das BMVBW hat in seiner Stellungnahme zu diesen Änderungsvorschlägen mitgeteilt, daß es im Rahmen der nächsten einschlägigen Novellierung lediglich zu § 61 Abs. 4a FeV (Abruf im automatisierten Verfahren aus dem VZR) eine neue Formulierung anstreben wird. Da mich die Argumente gegen die übrigen Änderungsvorschläge nicht überzeugt haben, werde ich versuchen, das Ministerium für weitere Änderungen zu gewinnen.

28.1.2 Fahrzeugpapiere bald ohne Geburtsdatum?

Bereits in meinem 14. TB (Nr. 18.5) hatte ich darauf hingewiesen, daß die – vielen Betroffenen unangenehme – Angabe des **Geburtsdatums** weder im Fahrzeugbrief noch im Fahrzeugschein erforderlich ist, weil sie nicht dem Zulassungszweck dient und für eine evtl. erforderliche Identifizierung des Halters andere Dokumente

Abbildung 16 (zu Nr. 28.1)

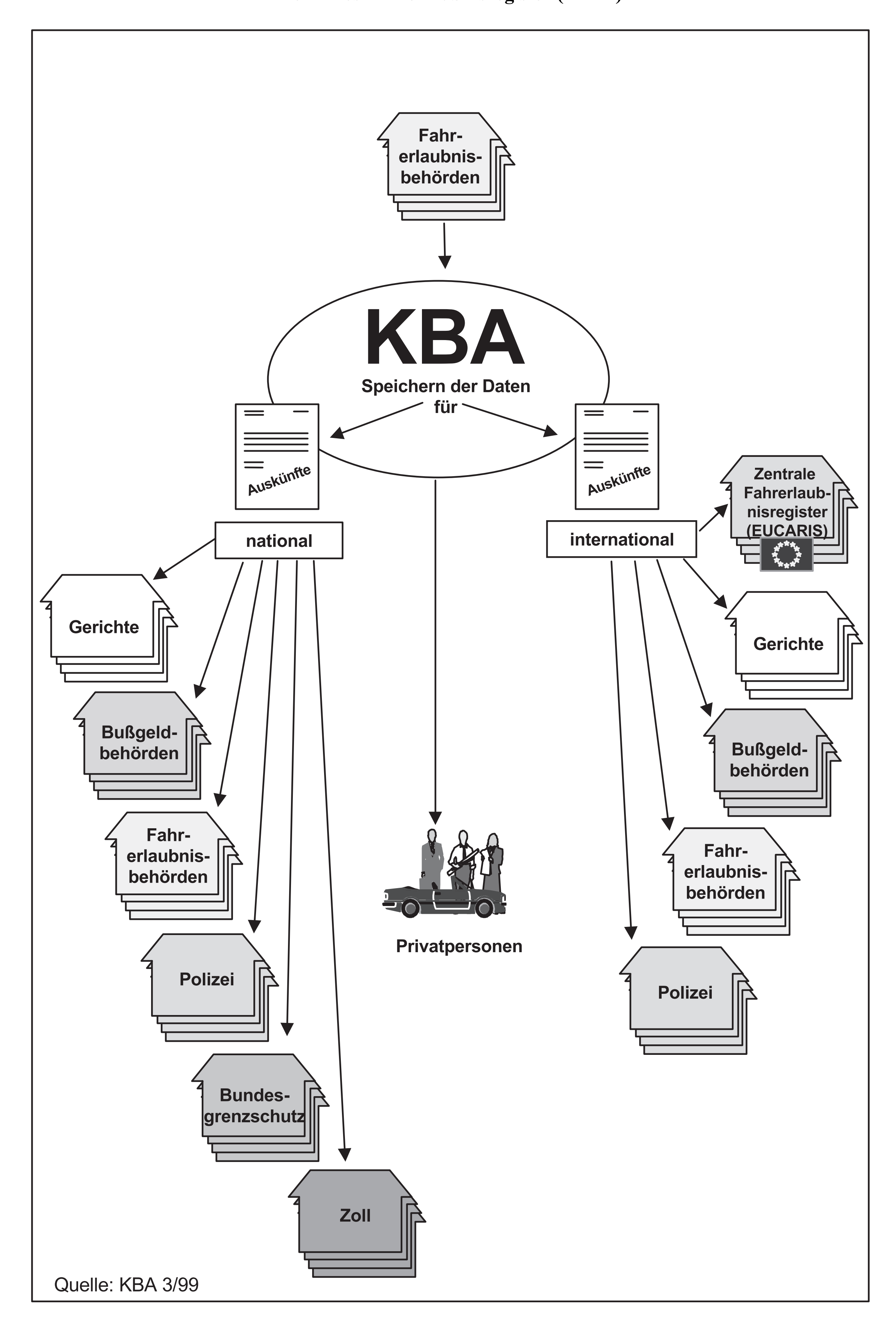
Zentrales Fahrzeugregister (ZFZR)



Quelle: KBA 3/99

Abbildung 17 (zu Nr. 28.1)

Zentrales Fahrerlaubnisregister (ZFER)



Quelle: KBA 3/99

zur Verfügung stehen. Erfreulicherweise enthält der europäische Richtlinienvorschlag über Zulassungsdokumente für Kraftfahrzeuge und Kraftfahrzeuganhänger (Kom (97) 248 endg.; Ratsdok. 8840/97) weder für die Zulassungsbescheinigung Teil I (Fahrzeugschein) noch für die Zulassungsbescheinigung Teil II (Fahrzeugbrief) diese Angabe (vgl. Anhang I Abschnitt V und Anhang II Abschnitt VI). Nach meinen Gesprächen mit dem BMVBW über eine richtlinienkonforme Änderung der Straßenverkehrs-Zulassungs-Ordnung gehe ich von seiner Bereitschaft aus, das Geburtsdatum im Rahmen der Anpassung der deutschen Fahrzeugpapiere an die in Kürze zu erwartende Richtlinie entfallen zu lassen.

In diesem Zusammenhang weise ich darauf hin, daß vermutlich noch weitere nationale Vorschriften im Zuge der europäischen Harmonisierung auf dem Prüfstand stehen werden.

Gerade weil der Datenschutz gelegentlich für einen höheren Verwaltungsaufwand verantwortlich gemacht wird, war es in diesem Fall für mich ermutigend, daß der Datenschutz zu Vereinfachungen für die Bürger und die Verwaltung beitragen konnte.

28.1.3 Neue Techniken für den Umgang mit Zulassungsdaten

Zwischen den Zulassungsbehörden und dem KBA sollen Zulassungsdaten künftig grundsätzlich nur über Magnetbandkassette, Magnetband, Diskette oder durch automatisierte Datenübertragung übermittelt werden. Dafür habe ich empfohlen, generell sowohl eine **Verschlüsselung** als auch **digitale Signaturen** vorzuschreiben, sobald die entsprechende Technik – auch zu vertretbaren Kosten – zur Verfügung steht. Für **elektronische Datenträger** erscheint dem BMVBW der mit einer Verschlüsselung der Daten und/oder einer digitalen Signatur verbundene Aufwand im Verhältnis zur erreichbaren Risikominderung noch zu hoch. Das Lesen oder Manipulieren von Datenträgern setze nämlich stets das Vorhandensein entsprechender Technik voraus. Deshalb sei die Gefahr, daß die auf den Datenträgern gespeicherten Informationen an nicht berechtigte Personen gelangen, geringer einzustufen als beim Versand auf Papierbelegen. Darüber hinaus existierten derzeit keine herstellerübergreifenden Standards oder mit geringem Aufwand einsetzbare Produkte, die in die unterschiedlichen DV-Systeme integriert werden können. Aus diesen Gründen sollte nach Auffassung des Ministeriums zunächst auf die Verschlüsselung elektronischer Datenträger verzichtet werden.

Im Hinblick auf die sich zum Teil noch im Entwicklungsstadium befindlichen Verfahren zur Verschlüsselung und zur digitalen Signatur halte ich diese Beurteilung für eine Übergangszeit noch für vertretbar. Sobald hierfür aber eine ausgereifte Technik zur Verfügung steht, werde ich im Hinblick auf die nach dem jeweiligen Stand der Technik zu fordernden Sicherheitsmaßnahmen bei der Übermittlung personenbezogener Daten auch auf eine Anpassung der derzeitigen technischen Verfahren drängen. Erfreulicherweise erklärte sich das Ministerium bereit, für **Online-Datenübertragungen** schon jetzt eine Verschlüsselung vorzuschreiben.

Weiter in die Zukunft reichen Überlegungen einiger Kommunen, die **Kraftfahrzeugzulassung über das Internet** zu ermöglichen. Dafür müßten Teilbereiche des Zulassungsverfahrens durch Beleihung z. B. auf Autohäuser, verlagert werden. Die für die Kontrolle in diesem Bereich zuständigen Landesbeauftragten für den Datenschutz lehnen dieses Verfahren insbesondere wegen der mit einer „Vorverlagerung“ der Zulassung verbundenen Probleme sowohl bei der Identitätsprüfung des Halters, etwa durch Eröffnung des Zugriffs auf die Daten der Meldebehörden, als auch bei der Sicherung und Kontrolle der rechtmäßigen Nutzung der dann an die Beliehenen zu überlassenden Blankovordrucke, Dienststempel sowie Dienst- und Prüfplaketten derzeit ab. Auch wenn diese interessante Alternative des Zulassungsverfahrens wegen vieler technischer und rechtlicher Hindernisse (u. a. Gewährleistung der Sicherungsfunktion des Kfz-Briefes hinsichtlich des Eigentums an Kraftfahrzeugen) heute noch fern liegt, so sollte sie bei der Schaffung neuer zulassungsrechtlicher Regelungen gleichwohl als künftig möglich in die Überlegungen einbezogen werden.

Schon heute sind Rationalisierungen bei der Erfassung der Daten aus Zulassungsanträgen und bei weiteren vorbereitenden Arbeiten möglich. So könnten Antragsteller, die dazu bereit und von der Zulassungsbehörde für das Verfahren zuzulassen wären, den Antrag durchaus über das Internet an die Zulassungsbehörde senden, die nach einer positiven Vorentscheidung ein Kennzeichen reserviert und dem Antragsteller mitteilt. Dieser könnte dann mit den vorbereiteten Schildern, dem Kraftfahrzeugbrief und der Versicherungsbestätigung bei der Zulassungsbehörde die vorbereitete Zulassung durchführen lassen.

Für solche Verfahren wären folgende technisch-organisatorische Vorkehrungen zu treffen:

– Die Antragsdaten sind für die Übertragung auf den Verbindungswegen durch Verschlüsselung vor unbefugter Kenntnisnahme zu schützen.
– Eine zweifelsfreie Identifizierung und Authentifizierung der Kommunikationspartner ist sicherzustellen.
– Eine Abschottung der Antragsdaten vom Echtdatenbestand der Zulassungsbehörden ist durch entsprechende Sicherungsmaßnahmen, wie Zugangs- und Zugriffskontrolle (Firewall) und Protokollierungsverpflichtungen, sicherzustellen.
– Die Daten aus einem Antrag dürfen erst nach der Zulassung in den Echtdatenbestand übernommen werden

Dieses habe ich dem BMVBW mitgeteilt und darauf hingewiesen, daß eine darauf aufbauende neue Form des Zulassungsverfahrens die Abläufe deutlich straffen könnte, ohne die Sicherheit der Kfz-Zulassung zu mindern. Auch eine zeitlich begrenzte Reservierung des Wunsch-Kennzeichens ließe sich mit diesem Verfahren erreichen. Im Hinblick auf die Einheitlichkeit des Zulassungsverfahrens habe ich jedoch empfohlen, unter Beachtung der in den einzelnen Ländern vorgegebenen technischen Bedingungen Grundsätze für die Teilnahme an einem automatisierten Antragsverfahren zu erarbeiten

und mich daran wegen seiner datenschutzrechtlichen Bedeutung zu beteiligen.

28.1.4 Zweckfremde Nutzung der KBA-Register

Der Zweck der beim KBA geführten zentralen Register besteht u. a. darin,

- Personen in ihrer Eigenschaft als Halter von Fahrzeugen und deren Anschrift,
- Inhaber von Fahrerlaubnissen und Fahrlehrerlaubnissen, amtlich anerkannte Sachverständige und Prüfer sowie
- Personen, die Ordnungswidrigkeiten und Straftaten im Zusammenhang mit der Teilnahme am Straßenverkehr begangen haben,

zu registrieren, um Auskünfte über den jeweiligen Sachverhalt geben und evtl. erforderlich werdende verkehrsbezogene Verwaltungs- und Ahndungsmaßnahmen (u. a. auch aufgrund durchgeführter Kontrollen) ergreifen zu können.

Nach der Änderung des StVG darf der jeweilige Datenbestand der einzelnen Register beim KBA zusätzlich sowohl zur Beseitigung von Zweifeln an der Identität einer eingetragenen Person als auch zum Abgleich zwischen den einzelnen Registern genutzt werden, um Fehler und Abweichungen festzustellen sowie Datenbestände zu vervollständigen. Gegen den Abgleich und eine damit mögliche Verknüpfung sämtlicher beim KBA gespeicherter Daten hatte ich im Rahmen meiner Beteiligung Bedenken geltend gemacht, weil auf diesem Wege ein zentrales Ersatz-Bundesmelderegister entstehen könnte. Die jeweiligen Vorschriften tragen jetzt diesen Bedenken dadurch Rechnung, daß sie zwar Abgleiche der Register untereinander zu den o.a. Zwecken vorsehen und neu erfaßte Angaben auch mit den für andere Zwecke bereits gespeicherten Daten verglichen werden dürfen, um Fehler bei der Erfassung zu erkennen und ggfs. berichtigen zu können. Die Zusammenfassung aller Erkenntnisse und ihre gemeinsame Verwendung für jeden Zweck ist jedoch erfreulicherweise nicht zugelassen.

Die gesetzlichen Ausnahmen von der Zweckbindung der Daten sind im Verhältnis zu den theoretischen Nutzungsmöglichkeiten eng begrenzt. Ein Beispiel dafür ist die zugelassene Nutzung der Register zur Feststellung von Halteranschriften, um auch die öffentlich-rechtlichen Ansprüche in Höhe von jeweils mindestens 1 000 DM geltend machen zu können, die nicht im Zusammenhang mit der Teilnahme am Straßenverkehr entstanden sind. In diese Regelung wurden privatrechtliche, aber auf die öffentliche Hand übergegangene **Unterhaltsansprüche** einbezogen. Daß diese Erweiterung gerechtfertigt ist, belegt eine Erhebung des KBA, nach der im 1. Halbjahr nach Inkrafttreten der Änderung mehr als 2 000 Anfragen gestellt wurden und bei fast jeder dritten Anfrage eine passende Halterauskunft erteilt werden konnte. Hinter den Anfragen standen Forderungen in Höhe von ca.10 Millionen DM, von denen der Staat nach Feststellung der neuen Anschrift der Unterhaltsverpflichteten etwa 2,5 Millionen DM zurückbekommen kann. Die Zulassung immer weitergehender Zweckänderungen könnte aber dazu führen, daß Personen, die – aus welchen Gründen auch immer – bestimmte Daten dem Staat nur zu einem bestimmten Zweck anvertrauen möchten, Umgehungen suchen, um solchen Nutzungen auszuweichen, z. B. durch Zulassung ihres Fahrzeuges auf eine andere Person. Dieses würde den Wert der Register erheblich mindern. Daher sollte bei jeder gesetzlich zugelassenen Zweckänderung auch dieser Gesichtspunkt berücksichtigt werden.

28.1.5 Grenzenlose Übermittlung von KBA-Daten?

Bei der Erarbeitung von Staatsverträgen mit ausländischen Staaten über den Austausch von Fahrzeug- und Halterdaten werde ich beteiligt. Hier wurde in letzter Zeit jedoch die Tendenz erkennbar, die nationalen Zweckbindungsregelungen bei der Übermittlung dieser Daten ins Ausland zu erweitern (z. B. für Zwecke der Gefahrenabwehr und zur Kriminalitätsbekämpfung), weitergehende Datenübermittlungen als national zugelassen zu fordern und die nationalen Sicherungsmaßnahmen unbeachtet zu lassen. Dieses würde den bereichsspezifischen Regelungen des StVG für **Datenübermittlungen ins Ausland** widersprechen. Auch mußte ich bei meinen Stellungnahmen zu Entwürfen von Staatsverträgen darauf hinweisen, daß bei der Zulassung von Online-Übermittlungen an ausländische empfangsberechtigte Stellen nur der Datenbestand bereitzustellen ist, der nach den nationalen gesetzlichen Regelungen durch Abruf im automatisierten Verfahren ins Ausland übermittelt werden darf.

Versuche, die von dem Gesetzgeber aus guten Gründen beschlossenen nationalen Zweckbindungs- und Übermittlungsregelungen für die Daten des KBA durch bilaterale Verträge oder europäische Übereinkommen mit nicht verkehrsspezifischer Zielrichtung aufzuweichen bzw. für bestimmte Zwecke außer Kraft zu setzen, halte ich nicht für die geeigneten Schritte auf dem Weg zu einer internationalen Harmonisierung. Wenn allerdings die praktische Anwendung der gesetzlichen Regelungen zeigen sollte, daß eine Erweiterung der zweckfremden Nutzung aus nachvollziehbaren Gründen erforderlich ist, dann müßte der Gesetzgeber die entsprechenden Regelungen auch für das Inland dem Bedarf anpassen.

28.1.6 Neue Regelungen zum Güterverkehr

Im Berichtszeitraum wurde ich u. a. an Gesetzesänderungen

- zum Güterkraftverkehrsgesetz,
- zum Gesetz über die Beförderung gefährlicher Güter und
- zum Fahrpersonalgesetz

beteiligt, die bereichsspezifische Regelungen zum Datenschutz enthalten.

Bei der Änderung des **Güterkraftverkehrsgesetzes** konnte erreicht werden, daß

- die Speicherung und Nutzung von Unternehmer- und Fahrerdaten nur für die im einzelnen festgelegten Zwecke erlaubt ist,

– Übermittlungen an die zuständigen Behörden nur zur Erfüllung der im Gesetz genannten Aufgaben zugelassen sind und
– angemessene Löschungsfristen festgelegt wurden.

Ich begrüße, daß inzwischen Entwürfe der im Güterkraftverkehrsgesetz vorgesehenen Erlaubnisverordnung und Allgemeinen Verwaltungsvorschrift für den Güterverkehr vorliegen, die Datenerhebungen und –übermittlungen nur in dem Umfang vorsehen, der sich im Jahre 1995 in Gesprächen mit dem damaligen BMV und dem **Bundesamt für Güterverkehr** (BAG) als ausreichend ergeben hat. Vor allem sollen den vor Erteilung einer Erlaubnis für den gewerblichen Güterverkehr zu beteiligenden Stellen nur noch die Angaben und Unterlagen übermittelt werden, die sie für die Beurteilung des Unternehmens benötigen.

Beim BAG habe ich mich über das dort eingeführte Unternehmensverwaltungssystem informiert und Hinweise zum Speicherungsinhalt sowie zum Verfahren geben können.

In das **Gesetz über die Beförderung gefährlicher Güter** sowie in das **Fahrpersonalgesetz** wurden Regelungen aufgenommen über

– den Datenverkehr mit den zuständigen Behörden der Mitgliedstaaten der EU und anderer Vertragsstaaten des Abkommens über den Europäischen Wirtschaftsraum (EWR) und
– die Speicherung, Nutzung und Übermittlung von Daten über abgeschlossene Bußgeldverfahren durch die Erlaubnisbehörden und das BAG (Beurteilung der Zuverlässigkeit von Unternehmen) sowie durch die Bußgeldbehörden zur Verfolgung weiterer Ordnungswidrigkeiten.

Dadurch konnten einheitliche Regelungen für die Speicherung und Nutzung von Unternehmer- und Fahrerdaten – von fachlich gebotenen Unterschieden einmal abgesehen – für die gesamte Güterverkehrsverwaltung erreicht werden.

Die **Verordnung (EG) Nr. 2135/98 des Rates** vom 24. September 1998 ändert die bisherigen EG-Regelungen über das **Kontrollgerät** zur Einhaltung der Lenk- und Ruhezeiten im gewerblichen Güter- und Personenverkehr. Danach müssen Fahrzeuge, die 24 Monate nach Inkrafttreten dieser Verordnung (9. Oktober 1998) zugelassen werden, mit einem elektronischen Kontrollgerät ausgerüstet werden. Die Regelung wurde gegen die Stimme Deutschlands beschlossen. Sie ist jedoch auch in Deutschland unmittelbar geltendes Recht.

In meiner Stellungnahme habe ich mich insbesondere gegen die lückenlose Aufzeichnung über alle Aktivitäten der Fahrer auf ihrer (noch einzuführenden) Fahrerkarte und im Kontrollgerät des Fahrzeuges ausgesprochen, da dieses Verfahren zu einer in diesem Umfang einmalig intensiven Überwachung der Berufstätigkeit führen würde. Ich habe darauf hingewiesen, daß bei einem derart schwerwiegenden Eingriff in die Rechte einer Berufsgruppe die Erforderlichkeit der Einführung dieses Aufzeichnungsmediums und der Verwendung der mit Hilfe dieser Einrichtungen gespeicherten personenbezogenen Daten im Prinzip und im Detail sorgfältig zu prüfen und zu begründen ist. Weder diese Darlegung noch mein Hinweis auf den in Artikel 6 der europäischen Datenschutzrichtlinie 95/46/EG vom 24. Oktober 1995 enthaltenen Rechtsgedanken der Datenvermeidung und Datensparsamkeit konnte dem Ministerium, das meine Auffassung insoweit teilte, zu einem Erfolg im Rat (Zurückstellung und eingehende Prüfung des Verfahrens, evtl. durch einen Feldversuch) verhelfen.

Bedauerlich ist auch, daß die Verordnung keine Regelungen zur Begrenzung der Datennutzung enthält. Auch wenn der Rat der Einhaltung von Lenk- und Ruhezeiten im Interesse der Verkehrssicherheit zu Recht einen hohen Stellenwert zumißt, hätte doch gerade bei einer so intensiven Überwachung eine Beschränkung der Datennutzung auf diesen Zweck erfolgen sollen. Dieser Mangel kann durch nationale Regelungen nur schwer ausgeglichen werden.

28.2 Kontrolle der ZEVIS-Nutzung beim Zollkriminalamt

Die Zollfahndungsdienststellen sind berechtigt, Abrufe aus dem Zentralen Verkehrsinformationssystem (ZEVIS) *„zur Verfolgung von Steuer- und Wirtschaftsstraftaten“* durchzuführen (§ 36 StVG). Ein ZEVIS-Abruf ist danach nur zulässig, wenn Anhaltspunkte dafür vorliegen, daß die erfragten Daten zur Klärung oder Verhinderung von Steuer- und Wirtschaftsstraftaten erforderlich sind. Außerdem dürfen Abrufe durch den Zoll erfolgen, *„soweit er grenzpolizeiliche Aufgaben wahrnimmt“*.

Bei einer **Kontrolle und Beratung des Zollkriminalamtes** (ZKA) habe ich festgestellt, daß das ZKA ZEVIS auch für nicht gesetzlich zulässige Zwecke nutzt. Zwei Beispiele mögen dies verdeutlichen:

– **Öffentlicher Parkraum** ist nicht nur in der Kölner Innenstadt rar, sondern wohl auch in Köln-Dellbrück. Die Anwohner der ehemaligen belgischen Kaserne hatten sich daran gewöhnt, daß bestimmte Parkflächen für sie reserviert zu sein schienen; diese wurden jedenfalls nicht von Ortsfremden benutzt. Nachdem das ZKA in diese ehemalige Kaserne eingezogen war, war es mit dem traumhaften Alleinbenutzungsrecht vorbei. Einige Mitarbeiter des ZKA nutzten diese Parkplätze nämlich, um nach Dienstschluß dem Gedränge am Haupteingang zu entgehen. Das war den parkraumverwöhnten Anwohnern ein Dorn im Auge und sie beschwerten sich bei der Präsidialstelle des ZKA unter Nennung des Kfz.-Kennzeichens. Da das ZKA nach dessen Auskunft *„aus Datenschutzgründen“* keine Datei über die Fahrzeuge der in die Liegenschaft einfahrberechtigten Mitarbeiter führt, waren seiner Meinung nach ZEVIS-Abfragen erforderlich, um die Halter *„wegen dringender Benachrichtigung im Zusammenhang mit seinem Kfz“* festzustellen. Dem ZKA war mit Sicherheit bekannt, daß ZEVIS-Abfragen für diesen Zweck unzulässig waren, es wollte wohl aber der guten Nachbarschaft wegen den vermutlichen Mitarbeiter anhalten, auf die Benutzung

des öffentlichen Parkraums zu verzichten. Diese mißbräuchliche ZEVIS-Nutzung habe ich **beanstandet**.

– **Die Sicherung der Liegenschaft** des ZKA ist erforderlich; deshalb erfolgt auch eine Kontrolle durch einen hierfür engagierten Wachdienst. Die Art und den Umfang der Kontrollmaßnahmen bestimmt die Dienststelle bzw. die hierfür zuständige Stelle. Nun liegt es in der Natur der Sache, daß langjährige Mitarbeiter nach Vorzeigen des Dienstausweises in die Liegenschaft einfahren, wenn kein Wachpersonal an der Schranke steht, um den Dienstausweis genau zu kontrollieren. Erfahrungsgemäß können Handzeichen des sich im Wachhäuschen befindlichen Wachpersonals mißverstanden werden, vor allem, wenn bestimmte Lichtverhältnisse Spiegelreflektionen verursachen. Dieses war wohl die Ursache dafür, daß, wie mir das ZKA mitteilte, in einigen Fällen eine *„Mißachtung des Haltegebots an der Wache zum Sicherheitsbereich“* unterstellt wurde.

  Die Angabe des ZKA, daß es zur Abwehr einer unmittelbar drohenden Gefahr möglicher Straftaten geboten war, auf schnellstmöglichem Wege Informationen über die eingefahrenen Halter zu erlangen, und dieses nur über die ZEVIS-Abfrage möglich war, ist nicht nachvollziehbar. Hätte wirklich eine unmittelbar drohende Gefahr bestanden, so hätte die Wache sofort gegenüber dem Fahrer und den eventuellen Mitbenutzern des Fahrzeuges einschreiten müssen. Die Feststellung des Halters über ZEVIS konnte zur Abwehr keinen entscheidenden Beitrag leisten, da wegen des Zeitverzuges (Anruf der Wache bei der Präsidialstelle, Anruf der Präsidialstelle beim Dauerdienst, Durchführung des Abrufs, Feststellung, ob der Halter Mitarbeiter des ZKA ist) eine unmittelbar drohende Gefahr so nicht hätte abgewendet werden können. Das ansonsten folgenlose Mißachten des Haltegebots konnte die Abrufe nicht rechtfertigten, sie waren gesetzwidrig. Wenn die Sicherheit der Liegenschaften eine schnelle Ermittlung der Kfz-Halter erfordert, muß die Dienststelle die hierfür erforderlichen Maßnahmen treffen (z. B. Anlegung einer Kennzeichen-Datei über die in die Liegenschaften einfahrberechtigten Kfz-Halter) und dieses mit der Personalvertretung vereinbaren. Datenschutzrechtliche Hinderungsgründe hierfür sind nicht erkennbar. Daß stattdessen ohne rechtfertigenden Grund ZEVIS in Anspruch genommen wurde, habe ich wegen Verstoßes gegen die durch § 36 Abs. 2 und 3 StVG festgelegten Beschränkungen **beanstandet**.

ZEVIS-Abrufe sind zu **protokollieren** (vergleiche § 36 Absätze 6 und 7 StVG). Hierfür haben die speichernden und abrufenden Stellen die erforderlichen organisatorischen und technischen Voraussetzungen zu schaffen (s. auch §§ 13 und 14 FRV). Darüber hinaus ist zu gewährleisten, daß die Zulässigkeit der Abrufe kontrolliert werden kann.

Bei meiner Kontrolle beim ZKA habe ich festgestellt, daß entgegen der mir bekannten Anordnung in der Praxis beim ZKA in den von dort geführten Aufzeichnungen

– Eintragungen, auch zu Anfragen mit Personendaten, fehlten und

– Eintragungen sowohl hinsichtlich der anfragenden Stelle als auch der verantwortlichen Person unvollständig waren bzw. statt der verantwortlichen Person der Beamte des Dauerdienstes beim ZKA benannt war.

Diese Mängel bei der Protokollierung von ZEVIS-Abrufen habe ich wegen Verstoßes gegen die durch § 14 Abs. 2 und 3 FRV festgelegten Verpflichtungen **beanstandet**.

Die Verantwortung der abrufenden Stelle und der fachaufsichtsführenden obersten Bundesbehörde, ZEVIS-Abrufe von ihrer Dienststelle oder innerhalb ihres Geschäftsbereichs nur für gesetzlich zulässige Zwecke zuzulassen, kann im nachhinein nur durch Kontrollen wahrgenommen werden. Da diese weder durch das ZKA noch durch das für die Fachaufsicht des ZKA zuständige BMF erfolgten, habe ich diese Unterlassung einer erforderlichen Sicherungsmaßnahme (Verstoß gegen § 36 Abs. 5 Nr. 2 StVG) **beanstandet**.

Die Notwendigkeit für aussagefähige Aufzeichnungen ergibt sich nicht nur für die Abrufe, für die eine Zusatzprotokollierungen erforderlich ist, sondern auch für die übrigen Abrufe, denn auf andere Weise kann das ZKA die Zulässigkeit der Abrufe nicht belegen und die gesetzlich vorgesehenen Kontrollen durch das ZKA selbst, die fachaufsichtsführende oberste Bundesbehörde oder durch meine Dienststelle wäre nicht möglich. Denn bei großen Dienststellen mit einem heterogenen Aufgabenzuschnitt und bei Abrufen durch eine Zentralstelle (Dauerdienst) ohne Aufzeichnung sämtlicher Abrufe kann nicht mehr nachvollzogen werden, welchen konkreten Zwecken die Abrufe dienten. Im übrigen kommt nach der Änderung der Fahrzeugregisterverordnung (§ 14 Abs. 4) hinzu, daß ab 1. Januar 1999 statt bisher für 2 % nunmehr für 10 % der Abrufe Zusatzprotokollierungen vorzunehmen sind und der Dauerdienst deswegen zur Vermeidung zeitraubender Rückfragen nach der automatisierten Aufforderung zur Zusatzprotokollierung über diese Angaben ohnehin verfügen muß. Die Vollprotokollierung erfordert unter diesen Voraussetzungen keinen wesentlichen Mehraufwand. Die Notwendigkeit hierzu würde jedoch entfallen, wenn die Abrufe von personengebundenen oder organisatorisch zuzuordnenden Terminals erfolgen.

Ergänzend zu Fragen der sachgerechten Protokollierung werde ich mit dem ZKA erörtern, welche sonstigen Maßnahmen ergriffen werden müssen, um in Zukunft unberechtigte Abrufe zu verhindern. Verbesserungen des Verfahrens sind auch deshalb erforderlich, weil nach der Statistik über durchgeführte Auswahlprotokollierungen im Jahr 1998 bei mindestens jedem 3. Abruf als Grund der Abfrage „sonstige Anlässe“ angegeben wurde. Angesichts der klaren gesetzlichen Vorgaben für die konkrete Angabe der Abrufgründe erscheint mir diese Praxis bedenklich.

Die Stellungnahme des BMF lag bei Redaktionsschluß noch nicht vor.

28.3 Luftverkehr

28.3.1 Neue luftverkehrsrechtliche Regelungen

Fast hätte ich den Stoßseufzer „Was lange währt, . . .“ ausgerufen, als nach langen und schwierigen Verhandlungen mit dem damaligen BMV endlich am 28. August 1998 das 11. Gesetz zur Änderung des Luftverkehrsgesetzes (LuftVG) verkündet wurde. Damit ging ein vierzehnjähriges Tauziehen um die Erforderlichkeit für bereichsspezifische registerrechtliche Regelungen im Luftverkehr zu Ende, in dessen Verlauf sogar der Deutsche Bundestag mit Beschluß vom 22. Juni 1995 verlangt hatte, einen Gesetzentwurf mit bereichsspezifischen Datenschutzregelungen für die Erhebung, Verarbeitung und Veröffentlichung von personenbezogenen Daten im Zusammenhang mit der Vorbereitung und Abwicklung des Flugverkehrs vorzulegen.

Das **Luftverkehrsgesetz** enthält durch Ergänzung um einen Vierten Abschnitt nunmehr ausgewogene Regelungen über die Einrichtung von Luftfahrtdateien und deren Zwecke, den Umfang der Speicherung personenbezogener Daten sowie über deren Übermittlung an festgelegte Stellen zu deren Aufgabenerfüllung. Nach dem LuftVG gibt es folgende Luftfahrtdateien:

- Luftfahrzeugregister (Datei der Verkehrszulassungen, die die Luftfahrzeugrolle und das Luftsportgeräteverzeichnis enthält),
- Zentrale Luftfahrerdatei (Datei der erteilten Erlaubnisse und Berechtigungen),
- Luftfahrer-Eignungsdatei (Datei der negativen Entscheidungen zu den erteilten Erlaubnissen und Berechtigungen sowie luftverkehrsrechtlich relevante Entscheidungen der Gerichte),
- Deliktsregister (Ordnungswidrigkeiten oder sonstige negative Entscheidungen über das Personal oder die verantwortlichen Personen von Unternehmen der Luftfahrt) und das
- Hauptflugbuch (Start und Landung von Luftfahrzeugen).

Hervorzuheben ist, daß eine Veröffentlichung von Daten aus der Luftfahrzeugrolle nur noch mit Zustimmung des Halters (ohne Eigentümerdaten) zulässig ist und trotzdem die erforderlichen Daten entsprechend dem Abkommen über die Internationale Zivilluftfahrt vom 7. Dezember 1944 an die darin genannten Stellen und an die Europäische Organisation für Flugsicherung (EUROCONTROL) für deren Zwecke übermittelt werden dürfen. Darüber hinaus konnte erreicht werden, daß Auskünfte an den Betroffenen über die zu seiner Person gespeicherten Daten entsprechend § 19 Abs. 7 BDSG nunmehr auch in der Luftfahrtverwaltung unentgeltlich erteilt werden.

Auch die von mir gegenüber dem damaligen BMV immer wieder angemahnte gesetzliche Regelung über die Erhebung, Verarbeitung und Übermittlung der Daten, die bei Flugunfalluntersuchungen entstehen (vgl. 15. TB Nr. 18.6), ist nunmehr durch Inkrafttreten des **Gesetzes über die Untersuchung von Flugunfällen** am 1. September 1998 zu einem positiven Abschluß gekommen. Damit sind der Umfang der zu erhebenden besonders schützenswerten Flugunfalldaten, die auch für die Verhütung künftiger Unfälle von erheblichem Nutzen sein können, sowie die Empfänger dieser Daten und die Übermittlungszwecke gesetzlich festgelegt.

28.3.2 Datenaustausch Luftsicherheit

Die Gewährleistung und Verbesserung der Luftsicherheit ist, wie Flugzeugunfälle immer wieder erschreckend verdeutlichen, eine wichtige Staatsaufgabe, die nicht hoch genug eingeschätzt werden kann. Diesem Ziel dient u. a. die Luftaufsicht, die im wesentlichen von den Luftfahrtbehörden der Länder wahrgenommen wird. Durch eine Ergänzung des Gesetzes über das Luftfahrt-Bundesamt (LBA) wird dieses Amt ab 1. März 1999 generell ermächtigt, neben der Kontrolle im Rahmen der von ihr erteilten Genehmigungen (Unternehmensgenehmigungen, Strecken- und Betriebsgenehmigungen für den Fluglinienverkehr, Einflugerlaubnisse) auch stichprobenweise Kontrollen des technischen und betrieblichen Zustandes von Luftfahrzeugen (sog. Ramp Checks) durchzuführen. Die Ergebnisse der Kontrollen durch die Luftaufsicht der Länder und der vom LBA für den o.a. Zweck eingerichteten Sicherheitsgruppe (Task Force) sollen – nach schrittweisem Aufbau – in einem Informationsverbund zwischen BMVBW, LBA, Luftaufsicht der Länder, Deutsche Flugsicherung GmbH (DFS – einschl. EUROCONTROL –), Flughafenkoordinator und Flughafenunternehmen gespeichert werden und diesen Stellen zur Erfüllung ihrer Aufgaben zur Verfügung stehen. Strittig ist innerhalb der Bundesregierung noch, ob die Übermittlung der im System gespeicherten personenbezogenen Daten durch § 15 BDSG gedeckt ist oder ob es für deren Erhebung, Speicherung und Übermittlung im automatisierten Verfahren einer besonderen gesetzlichen Grundlage bedarf. Die Beurteilung wird auch davon abhängen, ob die personenbezogenen Daten sich nur auf sicherheitskritische Feststellungen beziehen oder ob damit ein allgemeines Beobachtungssystem geschaffen werden soll, bei dem die im einzelnen registrierten Daten nicht im unmittelbaren Bezug zur Luftsicherheit stehen.

Gegen die Errichtung dieses Kommunikations- und Informationssystems Luftsicherheit (KISLS), das zu einer schnellen und umfassenden Information der mit den Aufgaben der Luftsicherheit befaßten Stellen beiträgt, habe ich keine Bedenken erhoben. Ich habe das damalige BMV jedoch darauf hingewiesen, daß durch organisatorische und technische Maßnahmen eine zweckfremde Nutzung dieser für Zwecke der Luftaufsicht verarbeiteten personenbezogenen Daten ausgeschlossen werden muß. KISLS wurde inzwischen in einem Teilbereich in Betrieb genommen.

Daß der Informationsverbund auch auf einen internationalen Datenaustausch abstellt, zeigt bereits die Einbeziehung von EUROCONTROL. Bestandteil von KISLS ist

aber auch das von der Europäischen Zivilluftfahrt Konferenz entwickelte Programm über die Sicherheitsuntersuchung für ausländische Luftfahrzeuge (Safety assessment of foreign aircraft – SAFA), nach dem die Ergebnisse der Ramp Checks einschließlich personenbeziehbarer Daten in sog. Reports formularmäßig erfaßt und den nationalen SAFA-Koordinatoren über die JAA (Joint Aviation Authorities) zur Verfügung gestellt werden. Auch auf EU-Ebene wurde das Thema „Luftverkehrs-Sicherheit" aufgegriffen. Der Richtlinienvorschlag der Europäischen Kommission über eine Sicherheitsüberwachung von Flugzeugen aus Drittstaaten, die auf Flughäfen der Gemeinschaft landen, greift das SAFA-Verfahren auf, indem er dieses Verfahren für die Mitgliedstaaten der EU verbindlich vorschreibt.

Wegen der engen Verflechtung der verschiedenen Institutionen und Informationsströme halte ich eine Harmonisierung sowohl auf nationaler als auch auf europäischer Ebene für geboten. Das Ziel muß sein, den für die Luftsicherheit zuständigen Stellen durch unterschiedliche Zugriffsrechte auf die Systeme die für ihre jeweilige Aufgabenerfüllung erforderlichen Daten verfügbar zu machen. Durch technische und organisatorische Maßnahmen ist die zweckfremde Nutzung auszuschließen und die Sicherheit der in diesem Zusammenhang verarbeiteten personenbezogenen Daten zu gewährleisten. Hier ist das Bundesministerium für Verkehr, Bau- und Wohnungswesen aufgerufen, innerhalb des luftrechtlich zulässigen Rahmens Standards zu setzen und im europäischen Rahmen an für die Mitgliedstaaten akzeptable Lösung mitzuarbeiten.

28.4 Wasserverkehr

28.4.1 Beabsichtigte Änderung des Binnenschiffahrtsaufgabengesetzes

Im Rahmen der vorgesehenen Neukonzeption des Verkehrsstatistikgesetzes war u. a. beabsichtigt, das Binnenschiffahrtsaufgabengesetz um bereichsspezifische Datenschutzregelungen zu ergänzen. Dabei sollten die aufgrund der Vorschriften des Gesetzes über die Statistik in der Binnenschiffahrt bestehende Schiffahrtsbestandskartei auf eine neue gesetzliche Grundlage gestellt und die Rechtsgrundlagen für weitere Dateien (Ordnungswidrigkeiten, Kleinfahrzeuge, Befähigungsnachweise) geschaffen werden. Die Ressortabstimmung des Referentenentwurfs, an dem ich auf der Fachebene frühzeitig beteiligt war, hat zu sachgerechten Ergebnissen geführt. Nachdem der Entwurf bis zum Ende der 13. Legislaturperiode von der Bundesregierung nicht abschließend beraten wurde, hoffe ich, daß die datenschutzrechtlichen Defizite nun bald beseitigt werden.

28.4.2 Beratung und Kontrolle der Wasser- und Schiffahrtsdirektion Nord

Bei einer Beratung und Kontrolle der Wasser- und Schiffahrtsdirektion Nord (WSD Nord) habe ich aufgrund verschiedener Eingaben auch das **Planfeststellungsverfahren** für die Anpassung der Fahrrinne der Unter- und Außenelbe an die Containerschiffahrt überprüft. Auch bin ich der Frage nachgegangen, ob in einem bestimmten **Beschwerdeverfahren** Daten in unzulässiger Weise von der WSD Nord oder von anderen Dienststellen im Bereich der WSD Nord gesammelt worden sind.

– Die Kontrolle des **Planfeststellungsverfahrens** zeigte, daß die Vorgehensweise fast durchweg datenschutzgerecht war, aber auch ein wesentlicher Fehler gemacht wurde:

  Zwischen der WSD Nord (Planfeststellungsbehörde) und dem Wasser- und Schiffahrtsamt Hamburg (Träger des Bauvorhabens) war vereinbart worden, daß die Eigentümerliste vor Erteilung des Druckauftrages aus dem Ordner „Vorläufiges Grunderwerbsverzeichnis" entsprechend den Regelungen der Planfeststellungsrichtlinie für die Wasser- und Schiffahrtsverwaltung des Bundes entfernt werde. Durch ein Versehen wurde das aber unterlassen mit der Folge, daß die beteiligten 125 Gemeinden, 181 Träger öffentlicher Belange sowie etwa 75 Verbände und Vereine auch die Eigentümerliste erhielten.

  Dieser Fehler wurde erst zwei Tage vor Offenlegung der Planfeststellungsunterlagen bei den Gemeinden bemerkt, worauf Mitarbeiter der WSD Nord sämtliche 125 betroffene Gemeinden telefonisch aufforderten, die Eigentümerlisten aus den Unterlagen zu entfernen und zu vernichten. Hinsichtlich der Träger öffentlicher Belange sowie der Verbände und Vereine war man jedoch der Auffassung, die Verzeichnisse könnten in den Unterlagen verbleiben, weil diese Exemplare nicht der Öffentlichkeit zugänglich, die Behörden und Verbände dem Datenschutz verpflichtet seien und somit personenbezogene Daten vertraulich zu behandeln hätten. Deshalb hatte man diesen Stellen keinen Hinweis auf die Eigentümerlisten gegeben, obwohl die übermittelnde Stelle nach § 15 Abs. 2 bzw. § 16 Abs. 2 BDSG die Verantwortung für die Zulässigkeit der Übermittlung personenbezogener Daten trägt und diese Verantwortung nicht stillschweigend den Trägern öffentlicher Belange und den Verbänden übertragen kann. So konnte nicht ausgeschlossen werden, daß Personen, die z. B. Mitglied eines Deichverbandes sind, durch die Beteiligung an diesem Verfahren von den Eigentumsverhältnissen der eventuell zu erwerbenden Grundstücke erfuhren. Die WSD Nord hätte durch rechtzeitige Information dieser Behörden und Verbände eine unzulässige Kenntnisnahme und Nutzung dieser personenbezogenen Daten durch Dritte verhindern können und müssen. Die unzureichende Reaktion auf den Fehler habe ich gegenüber dem BMV **beanstandet** (s. Anlage 3).

– Die Prüfung der Vorwürfe eines **Beschwerdeführers**, der vermutete, daß in seiner bei der WSD Nord geführten Dienstakte Daten über Ordnungswidrigkeiten über die zulässige Zeit hinaus verblieben sind und nicht gelöscht wurden, ergab keinen Hinweis auf die vermuteten Verstöße. Bei allen beteiligten Stellen war die Aktenführung sachgerecht und entsprach den datenschutzrechtlichen Anforderungen, so daß ich dem Beschwerdeführer mitteilen konnte, daß seine Besorgnisse unbegründet waren.

– Darüber hinaus habe ich festgestellt, daß die Arbeitsplatzbeschreibungen des **Datenschutzbeauftragten** und seines Vertreters keine Zeitanteile für die Erledigung der Datenschutzaufgaben enthielten. Bei Verfahren mit datenschutzrechtlichem Bezug war der Datenschutzbeauftragte auch nicht regelmäßig beteiligt worden, in dem o.g. Planfeststellungsverfahren erst bei Erarbeitung der Stellungnahme an meine Dienststelle.

Ich habe den BMVBW auf diesen Mangel hingewiesen.

29 Post

29.1 Neues Postgesetz in Kraft getreten

Am 1. Januar 1998 sind mit dem Inkrafttreten des neuen **Postgesetzes** (PostG) die Rahmenbedingungen für die Liberalisierung des Postdienstes festgelegt worden. Das Gesetz enthält Bestimmungen zur flächendeckenden Grundversorgung mit Postdienstleistungen zu erschwinglichen Preisen, zur Regulierung marktbeherrschender Anbieter sowie Regelungen zum Schutz des Postgeheimnisses und zum Datenschutz. Im Rahmen der Ressortabstimmung (s. 16. TB Nr. 29.1) und der parlamentarischen Beratungen habe ich mich an den Diskussionen des Gesetzentwurfs beteiligt. In mehreren Punkten sind meine datenschutzrechtlichen Anregungen im neuen Postgesetz berücksichtigt worden.

§ 39 des Gesetzes enthält die einfachgesetzliche Ausprägung des Postgeheimnisses, da die privaten Postdienstleister mangels grundrechtlicher Drittwirkung nicht unmittelbar an Artikel 10 des Grundgesetzes gebunden sind. § 41 PostG regelt die datenschutzrechtlichen Rahmenbedingungen, die von den Unternehmen beim geschäftsmäßigen Erbringen von Postdienstleistungen beachtet werden müssen, sowie die Ermächtigung der Bundesregierung, für diese Unternehmen durch Rechtsverordnung mit Zustimmung des Bundesrates Vorschriften zum Schutz personenbezogener Daten zu erlassen. Abweichend von § 38 BDSG überträgt § 42 Abs. 3 PostG dem BfD die datenschutzrechtliche Kontrolle von Unternehmen, soweit sie geschäftsmäßig Postdienstleistungen erbringen. Ich habe deshalb interessierte Postdienstunternehmen zu einer ersten Informationsveranstaltung eingeladen, um meine Beratung in Datenschutzfragen anzubieten und einen regelmäßigen Gesprächskreis zu Datenschutzfragen im Postsektor einzurichten. Die erste Gesprächsrunde, bei der auch die Regulierungsbehörde und das BMWi vertreten waren, hatte eine gute Resonanz, so daß ich zuversichtlich bin, daß künftig ein ständiger Gedankenaustausch zu Datenschutzfragen in diesem Bereich stattfinden wird.

Die Bundesregierung hat bisher von ihrer Ermächtigung, durch Rechtsverordnung neue Vorschriften zum Schutz personenbezogener Daten beim geschäftsmäßigen Erbringen von Postdienstleistungen zu erlassen, noch keinen Gebrauch gemacht, so daß weiterhin die Postdienstunternehmen-Datenschutzverordnung (PDSV) vom 4. November 1996 in Kraft ist. Durch das Nebeneinander von „alter“ Datenschutzverordnung und „neuem“ PostG hat es bereits in einigen Anwendungsfragen Probleme gegeben. So fehlt eine datenschutzgerechte Regelung zur Umsetzung der gesetzlichen Auflage an den Marktführer, den Mitbewerbern den Zugang zu seinen Informationen über Nachsendungsaufträge zu gestatten. Auch wegen der vielen neuen Postdienstleistungsunternehmen, die seit 1998 auf dem liberalisierten Markt für Postdienstleistungen tätig geworden sind, halte ich den Erlaß einer neuen PDSV für eine vordringliche Aufgabe.

29.2 Nachsendungsaufträge

29.2.1 „Unerwünschte Nebenwirkungen“ bei Nachsendungsaufträgen

In den vergangenen zwei Jahren habe ich in zunehmendem Maße Eingaben zu Fehlern und Problemen bei der Durchführung von Nachsendungsaufträgen durch die Deutsche Post AG erhalten. Zumeist beschwerten sich Postkunden über Fehler bei zeitlich befristen Nachsendungsaufträgen, die z. B. wegen eines Urlaubs gestellt wurden, aber Wochen danach die „unerwünschten Nebenwirkungen“ entfalteten, daß einige Korrespondenzpartner die Urlaubsanschrift als neue Wohnanschrift führten.

So wunderte sich ein Einsender, daß er zu Hause bei einem Arztbesuch – mehrere Wochen nach einem Sylt-Urlaub – nach dem Einlesen seiner Krankenversichertenkarte gefragt wurde, ob denn die neue Wohnanschrift auf Sylt die richtige sei. Zunächst konnte er sich nicht erklären, wie seine vorübergehende Urlaubsadresse seiner Krankenkasse fälschlicherweise als neue Wohnanschrift bekannt geworden sein könnte. Die zunächst angestellte Vermutung, die Anschrift sei irrtümlich zum Adressenabgleich „neu gegen alt“ an die Firma „Deutsche Post Adress GmbH“ weitergeleitet worden, bestätigte sich nicht, da Adressen aus Nachsendungsaufträgen vom Nachsendungsauftragszentrum der Deutschen Post AG nur dann weitergegeben werden, wenn es sich um einen Nachsendungsauftrag wegen Umzugs handelt und wenn der Auftraggeber die vorgedruckte Einwilligungserklärung zur Weitergabe nicht gestrichen hat. Adressen aus Aufträgen wegen vorübergehender Abwesenheit gibt das Auftragszentrum nicht an Dritte weiter. Allerdings besteht für den Absender eines Briefes die Möglichkeit, mit einer entsprechenden Vorausverfügung, z. B. dem Verlangen nach einer Anschriftenberichtigungskarte, eine Anschriftenänderung vom Zusteller mitgeteilt zu bekommen. Dabei muß der Zusteller die Regelungen beachten, die auch für das Nachsendezentrum gelten. Es kann jedoch vorkommen, daß der Zusteller am Wohnort versehentlich die nicht mitzuteilende, vorübergehende Urlaubsanschrift trotzdem weitergibt. Das ist vermutlich in dem o.a. Fall geschehen, und die Krankenkasse interpretierte daraufhin die mitgeteilte Anschrift als Umzugsanschrift und „korrigierte“ die vorhandenen Daten des Einsenders. Mit einem solchen Fehler können erhebliche Unannehmlichkeiten verbunden sein, denn der Betroffene erfährt zumeist erst im Laufe der Zeit durch eingehende Sendungen, welche Firmen und Behörden auf diesem Wege die falsche Anschrift erhalten haben.

Nach Angaben der Deutschen Post AG werden mit dem neuen Nachsendungsverfahren solche Fehler nicht mehr auftreten können, da dann die Anschriften nur noch durch die Nachsendezentren mitgeteilt werden. Dort sei die Weiterleitung einer vorübergehenden Anschrift als neue Anschrift technisch ausgeschlossen. Ich werde die Umstellung des Nachsendeverfahrens im Rahmen meiner Aufgaben begleiten und dabei insbesondere auf die Fehleranfälligkeit achten.

Häufig wurde bei Aufträgen zur Nachsendung wegen Umzugs der Hinweis auf die „Einwilligung in die Weitergabe der Umzugsdaten an Dritte“ und damit die Einwilligung in den Adressentausch „neu gegen alt“ übersehen, so daß die Umziehenden unwissentlich eingewilligt hatten und sich anschließend erstaunt an mich wandten, weil sie unter ihrer neuen Anschrift z. B. Versandhauskataloge erhielten, obwohl sie ihre neue Adresse diesen Unternehmen selbst nicht mitgeteilt hatten. Die Einwilligungsklausel wird auf dem Nachsendungsauftragsformular vor allem deshalb gelegentlich übersehen, weil sie relativ klein gedruckt und auf dem Formular zwar in Höhe der Unterschriftszeile, aber unterhalb der Ausfüllfelder am linken Formularrand plaziert ist. Der mitunter festzustellende Ärger von Einsendern über ihre ungewollte Einwilligung in die Weitergabe ihrer Umzugsanschrift an Dritte wird durch diese Art der Formulargestaltung der Post mitverursacht. Ich habe die Deutsche Post AG gebeten, durch eine deutlicher hervortretende Einwilligungsklausel mitzuhelfen, diese Irrtümer und den damit verbundenen Unmut der Betroffenen zu verringern.

29.2.2 Besuch des zentralen Nachsendungsauftragszentrums in München

Seit Herbst 1996 erprobt die Deutsche Post AG ihr neues **I**T-gestütztes **Na**ch- und Rücksendeverfahren (**INA**), in dem das zentrale Auftragszentrum in München sowie vier weitere Nachsendezentren mit den jeweiligen regionalen Briefverteilzentren zusammenwirken.

Im April 1997 habe ich das neue Verfahren im Auftrags- und Nachsendezentrum München kontrolliert. Für das INA-Verfahren hat die Deutsche Post AG ein neues Formblatt entwickelt, mit dem der Postkunde seinen Nachsendungsauftrag wegen Umzugs oder bei vorübergehender Abwesenheit erteilen kann. Diese Aufträge werden von der Post an das Auftragszentrum gesandt, dort erfaßt, bearbeitet und bei formaler und logischer Richtigkeit gespeichert. Die Daten der akzeptierten Aufträge sendet das Auftragszentrum an das jeweils zuständige Nachsendezentrum. In der Endausbaustufe von INA soll noch vor der Ausführung der akzeptierten Aufträge eine Auftragsbestätigung erstellt und über die Zustellstützpunkte an die Betroffenen gesandt werden (siehe auch Nr. 29.2.3). Damit können diese ihre Aufträge prüfen und ggf. stornieren oder korrigieren lassen.

Das Auftragszentrum druckt die Nachsendungsmerkkarten und schickt sie an die jeweiligen Postfilialen und Briefzentren, damit diese die Briefsendungen auftragsgemäß nachsenden können. Gleichzeitig gibt das Auftragszentrum die alte und neue Adresse des Umziehenden an die „Deutsche Post Adress GmbH“ zum Adressenabgleich „alt gegen neu“ weiter, sofern der Umziehende in die Weitergabe seiner Umzugsdaten an Dritte eingewilligt hat. In den Nachsendezentren laufen alle Briefsendungen auf, die vom Zusteller unter der alten Adresse nicht zugestellt werden können. Die Sendungen werden mit den vorliegenden Aufträgen aus dem Auftragszentrum abgeglichen. Je nach Ergebnis werden sie über das Briefverteilzentrum an die neue Anschrift dem Empfänger oder als Rücksendung dem Absender zugestellt. Die Frachtpostsendungen werden z.Z. noch an die alte Adresse gesandt, dort vom Zusteller handschriftlich mit der Nachsendungsadresse versehen und an den hierfür zuständigen Zustellstützpunkt weitergeleitet. Die Post erprobt aber bereits eine Verfahrensänderung, nach der die Frachtpostsendung direkt nach der Einlieferung auf einen vorliegenden Nachsendungsauftrag geprüft und dann direkt an die neue Anschrift gesandt werden kann.

Nach meinen Feststellungen ist sowohl das Verfahren INA als auch dessen Anwendung in München datenschutzrechtlich unbedenklich.

29.2.3 Pilotprojekt „Nachsendung Spezial“ datenschutzrechtlich begleitet

Im April 1998 habe ich durch eine Anfrage erfahren, daß die Deutsche Post AG ein Nachsendungsverfahren erproben will, das um eine Auftragsbestätigung und einen Umzugsratgeber erweitert ist. So soll nach Abgabe des Nachsendungsauftrages wegen Umzugs und Einwilligung des Umziehenden in die Weitergabe der Umzugsdaten an Dritte eine Auftragsbestätigung an die neue Anschrift des Auftraggebers gesandt werden, die dazu dient, die vor dem Umzug angegebene Anschrift zu verifizieren und bei Bedarf zu ergänzen oder zu ändern. Dies ist sinnvoll, wurde aber bisher aus Kostengründen unterlassen. Deshalb sieht das Pilotprojekt vor, der Auftragsbestätigung einen Umzugsratgeber beizulegen, der bei Einwilligung in die Weitergabe der Umzugsadresse an Dritte vorgedruckte Postkarten mit der neuen Absenderanschrift des Umgezogenen enthalten soll, mit denen er Werbepartnern der Post wie z. B. Versand- oder Möbelhäusern die neue Anschrift mitteilen und ggf. einen Katalog dieser Firma anfordern kann. Die Deutsche Post AG erläuterte, daß die bisher kostenlose Serviceleistung Nachsendung künftig nur noch gegen Entgelt oder auf Dauer nur dann entgeltfrei erbracht werden kann, wenn die Kosten durch zusätzliche Einnahmen, z. B. durch Werbung in einem mitgesandten Umzugsratgeber, erwirtschaftet werden.

Deshalb erprobt die Deutsche Post AG auch die Akzeptanz der entgeltlichen Abgabe eines Umzugssets, das neben dem Nachsendungsauftragsformular den Umzugsratgeber und Postwertzeichen im Wert von 20 DM enthalten soll. Nach Abgabe des Nachsendungsauftrages soll der Umgezogene mit der Auftragsbestätigung die mit seiner Anschrift vorgedruckten Postkarten nur dann erhalten, wenn er in die Adressenweitergabe vorher eingewilligt hat. Er kann – wie auch bei der entgeltfreien Version – selbst entscheiden, ob er die mit seiner neuen Anschrift bedruckten Karten an die vorgedruckten Unternehmen absendet.

Datenschutzrechtlich ist die Verifizierung der angegebenen Adresse, die sowohl als Nutzen als auch als Erheben von Bestands- oder Verkehrsdaten anzusehen ist, nach § 3 Abs. 1 bzw. 2 PDSV zulässig. Für die vorgedruckten Adressangaben wird von der Post eine Lösung angestrebt, die datenschutzrechtlich auf einem sicheren Fundament steht. Ich werde die Deutsche Post AG hierbei weiterhin beratend unterstützen.

29.3 ePost – eine neue Postdienstleistung

Die Deutsche Post AG bietet mit ihrem Geschäftsfeld **PostCom** vor allem Geschäftskunden wie Kreditinstituten, Versicherungen oder Versorgungsunternehmen den neuen elektronischen Briefservice und elektronischen Mehrwertdienst **ePost** an. Bisher gibt es ePost-Stationen in Hannover, Berlin, Duisburg, Frankfurt a.M., Leipzig und Nürnberg. Drei weitere Stationen sind in Hamburg, Stuttgart und München geplant.

29.3.1 Mit ePost werden aus Daten Briefe

PostCom bietet seinen Kunden an, aus Daten, die online über Internet oder offline auf Datenträgern (Magnetbänder, Disketten, CD) angeliefert werden, standardisierte Briefsendungen anzufertigen und zu versenden. Die Übernahme der Daten in das ePost-Verfahren erfolgt ohne Plausibilitätskontrollen oder inhaltliche Prüfungen, d. h. es wird gedruckt wie vom Auftraggeber vorgegeben. Der ePost-Station werden i.d.R. die Vordrucke/Formulare von den Kunden angeliefert. Die Vordrucke können farbig gestaltet und mit Firmenlogo, Grafiken, Unterschriftenfaksimiles versehen sein. In der Station werden aus den Daten körperliche Nachrichten, z. B. Rechnungen, Mahnungen oder Werbeschreiben, als Postsendungen erstellt. Die Sendungen werden gegenwärtig nur in schwarz gedruckt, die Schreiben werden nicht unterschrieben. Als Sendungsarten sind gewöhnliche Briefe im Format Standard, Kompakt, Groß und Maxi, Infobriefe, Infopost und Postkarten möglich. Die Sendungen sind durch einen auf dem Umschlag angebrachten Aufdruck von vornherein freigemacht. Die ePost-Stationen befinden sich stets in unmittelbarer Nähe zu einem Postverteilzentrum, so daß die Sendungen unmittelbar nach ihrer Herstellung ausgeliefert werden können.

Als ergänzende Dienstleistung bietet ePost den Kunden die Archivierung der Dateien auf CD an.

29.3.2 Kontrolle einer ePost-Station

Ich habe die Einführung des neuen ePost-Verfahrens zum Anlaß genommen, in einer Station das Verfahren zu kontrollieren.

In der Regel liefert der Kunde die für seine Sendungen benötigten Daten bei einer für ihn günstig gelegenen ePost-Station bereits nach Postleitzahlen sortiert ein, so daß später eine schnelle Zulieferung der im ePost-Verfahren gefertigten Sendungen an die Postverteilzentren möglich ist. Bei Wahl des online-Verfahrens werden die Daten über den Firewall-geschützten zentralen Zugang der Post in Darmstadt in das posteigene Telekommunikationsnetz übernommen und an die empfängernahen Stationen gesendet.

Für den Druck der Sendungen mit anschließendem oder vom Drucken getrenntem Kuvertieren sind mehrere Maschinenstraßen eingerichtet. Die Produktion wird aus einem Operatorenraum von Systemoperatoren überwacht, wobei das 4-Augen-Prinzip gilt. Die Operatoren können betriebsbedingt z. B. bei Störungen über die Terminals in den Arbeitsablauf eingreifen und dabei eventuell Kenntnis von den Kundendaten erhalten. Maschinenbedingte Störungen kommen manchmal beim Kuvertieren vor, so daß die Bedienkräfte an den Maschinen eventuell Kenntnis vom Inhalt der ePost-Sendung erhalten können. Außer diesen Operatoren sowie dem Produktions- und dem Stellenleiter haben keine weiteren Personen Zugriffsmöglichkeiten.

Die in der Station eingesetzten Datenträger werden nur auf Wunsch archiviert. Dies geschieht getrennt von der Produktion in einem zusätzlichen Lauf auf einer gesonderten Archivierungsstation. Die Archivierungsstation ist mit CD-Brenner ausgestattet, die Archivierung wird protokolliert. Je nach vertraglicher Vereinbarung mit dem Kunden werden die Datenträger regelmäßig gelöscht oder ungelöscht zurückgesandt oder abgeholt.

Der Produktionsleiter ist zugleich interner Datenschutzbeauftragter; bei Problemen steht auch der Datenschutzbeauftragte der Generaldirektion zur Verfügung. Gemäß § 15 Abs. 1 AGB ePost verpflichtet sich PostCom dazu, alle bei ihr für ePost gespeicherten Informationen über den Kunden, seine im ePost-System hinterlegten Druckvorlagen und deren Codes sowie die übermittelten Daten unter Beachtung des Post- und Fernmeldegeheimnisses sowie der PDSV i.V.m. dem BDSG vertraulich zu behandeln und in für Außenstehende nicht zugänglichen Räumen zu verarbeiten. Jeder Mitarbeiter wird bei Aufnahme seiner Tätigkeit in der Station auf das Datengeheimnis nach § 5 BDSG verpflichtet. Ebenso schriftlich verpflichtet werden Mitarbeiter von Fremdfirmen (Reinigungskräfte, Wartungspersonal). Darüber hinaus hat die PostCom festgelegt, keinen Subunternehmer einzuschalten sowie die ihr überlassenen Daten nicht Dritten zugänglich zu machen und auch nicht für eigene Zwecke zu nutzen.

Nach meinen Feststellungen gewährleistet sowohl das Verfahren als auch die Produktion der Sendungen der von mir kontrollierten ePost-Station den Datenschutz.

29.3.3 Warum ePost eine Postdienstleistung ist

Weil beim ePost-Verfahren auch personenbezogene Daten verarbeitet werden, ist es u. a. schon für die Vertragsgestaltung von Bedeutung, ob Teile dieser Dienstleistung als „Datenverarbeitung im Auftrag“ anzusehen sind oder die gesamte Dienstleistung eine Postdienstleistung ist.

Die Begriffsbestimmungen des am 1. Januar 1998 in Kraft getretenen neuen PostG sind auch im Hinblick auf kommende neue Postdienstleistungen weit auszulegen. Dies ergibt sich hinsichtlich des Postgeheimnisses aus

dem – nach der Gesetzesbegründung bewußten – Verzicht auf eine enumerative Abgrenzung des Schutzbereiches des Postgeheimnisses. Damit unterfallen der Inhalt von Postsendungen und die näheren Umstände des Postverkehrs im Interesse des Postkunden auch dann dem Postgeheimnis, wenn im Zuge neuer technischer Entwicklungen neuartige Postdienste angeboten werden. Unzweifelhaft unterfällt das Befördern adressierter schriftlicher Mitteilungen (Briefsendungen) vom Absender zum Empfänger dem Anwendungsbereich des PostG und damit dem Schutzbereich des Postgeheimnisses. „Befördern" umfaßt hierbei aber nicht nur den reinen Transportvorgang, sondern alle Elemente vom Annehmen oder Einsammeln, über das Bearbeiten und Weiterleiten bis zum Ausliefern an den Empfänger. Insoweit gehört schon die Übernahme der „Briefdaten" zum Zwecke der Übermittlung an den Empfänger mit zur Beförderungsleistung. Im Rahmen dieser Beförderungsleistung erfolgt zwar ein Medienbruch, denn die elektronisch gespeicherten Daten werden auf Papier ausgedruckt, anschließend gefaltet und kuvertiert. Eine inhaltsorientierte Datenverarbeitung, insbesondere eine Prüfung auf Plausibilität und Schlüssigkeit, findet jedoch nicht statt.

Die physikalische Transformation von der elektronischen Form von Anschrift und weiterem Nachrichteninhalt mit den vorgedruckten Formularen zu fertig einkuvertierten und frankierten Briefsendungen hat dabei keinen Einfluß auf die datenschutzrechtliche Bewertung. Eine ähnliche Transformation war schon immer Bestandteil der Nachrichtenbeförderung mit Telegrammen. Die Post wirkt dabei lediglich als Bote von Nachrichten. Der „Bote" ePost muß und soll im Normalfall nicht vom Inhalt Kenntnis erlangen. Läuft das Verfahren – hier das Drucken und Kuvertieren – fehlerfrei, so besteht wie bei der normalen Briefbeförderung genauso wenig die Möglichkeit, Kenntnis vom Inhalt der Briefe zu erhalten. Deshalb ist die Dienstleistung vom Annehmen der Daten bis zum Ausliefern der Sendungen als Postdienstleistung anzusehen.

Das Kuvertieren und Hinzufügen von Beilagen ist – technologisch bedingt – derzeit allerdings noch etwas störanfällig, und es treten in der Praxis Unterbrechungen auf, die ein manuelles Eingreifen erfordern. Die dabei für die Erbringung der Postdienstleistung nicht vermeidbare mögliche Kenntnisnahme vom Inhalt oder von der Anschrift unterliegt dem Postgeheimnis nach § 39 Abs. 3 PostG.

Das Archivieren im Auftrag ist nach meiner Auffassung eine dem eigentlichen ePost-Verfahren nicht immanente und zusätzliche Dienstleistung. Daher ist für diese eindeutige Auftragsdatenverarbeitung nach § 11 BDSG zu verfahren.

29.4 Die Postagentur im „Tante-Emma-Laden"

Durch ein neues Vertriebskonzept der Deutschen Post AG haben sich für den Bürger, vor allem, wenn er im ländlichen Raum wohnt, wesentliche Änderungen ergeben. Landauf landab hat die Deutsche Post AG ihr bisheriges Filialnetz ausgedünnt, weil viele dieser Filialen unrentabel waren. Gleichzeitig hat sie in den von Schließungen betroffenen Gebieten in großer Zahl Postagenturen in Einzelhandelsgeschäften eingerichtet, bis Ende 1997 insgesamt schon mehr als 5.200. Parallel zum Aufbau dieser neuen Struktur erhielt ich zunehmend Eingaben von Bürgern, die Sorge hatten, daß ihre vertraulichen Post- und Bankgeschäfte in Postagenturen nicht ausreichend geschützt würden. Ich habe mich deshalb über Aufgaben und Arbeitsabläufe bei mehreren Postagenturen im Köln-Bonner Raum informiert, die Einhaltung datenschutzrechtlicher Vorschriften kontrolliert und die Post beraten.

Bei den besuchten Postagenturen wurden sämtliche Postdienstleistungen, Postbankleistungen (Girodienst), Telefonkartenverkauf, Telefonbuchausgabe sowie die Telegrammaufgabe angeboten. Diese Agenturen waren alle in Zeitschriften- und Schreibwarengeschäften untergebracht. Die Wahl des Standortes der Posttheke innerhalb der Geschäftsräume war nicht immer optimal. In einer Agentur war sie im Durchgangsbereich aufgestellt, so daß auch andere Geschäftskunden mit dem Postbereich in Berührung kommen konnten. Eine gekennzeichnete **Diskretionszone** gab es in keiner Agentur. Weil der verfügbare Platz in einer Postagentur in der Regel eng begrenzt ist, läßt sich nicht jeder Wunsch verwirklichen, aber ein Hinweisschild oder eine Markierung könnte – auch in kleinen Geschäftsräumen – die Kunden zu mehr gegenseitiger Rücksichtnahme ermuntern.

Die in einer gelben Postkiste neben der Theke abgelegten Briefe waren teilweise einsehbar, so daß von der Kundenseite durchaus feststellbar war, wer mit wem in Briefkontakt steht. Ich habe der Post empfohlen, Briefe generell in einem nicht einsehbaren Bereich hinter der Theke aufzubewahren. Darüber hinaus stand in allen Agenturen ein Nebenraum zur Lagerung aufgegebener Päckchen und Pakete zur Verfügung, in dem die abends nach der turnusmäßigen Abholung noch angenommenen Briefe, Pakete und Päckchen über Nacht verschlossen aufbewahrt werden; nicht alle besuchten Agenturen waren jedoch alarmgesichert.

Soweit bei der Bereitstellung von Postdienstleistungen personenbezogene Daten verarbeitet wurden, waren die dabei eingesetzten Verfahren datenschutzrechtlich unbedenklich. Die Postagenturen sind mit dem Standard-DV-System der Post (EPOS) ausgestattet, bei dem Monitor und Drucker von der Kundenseite regelmäßig nicht einsehbar sind. Personenbezogene Daten werden bei Postbankleistungen, bei Einschreiben, Einschreiben mit Rückschein, Postzustellungsurkunden, Paketen, Expresspaket-Einlieferungslisten, Infopost-Empfängerlisten und bei Telegrammen erfaßt. Die Daten werden teils manuell und teils automatisiert bearbeitet. Im Postbank-Girodienst werden die automatisierten Daten (Auszahlung) von der Postbank einmal nachts abgerufen. Unterlagen über Aufzeichnungen (z. B. über Wertbriefe, benachrichtigte Sendungen etc.) verbleiben bei allen besuchten Postagenturen auch über Nacht – zumeist in verschlossenen Schubladen – in den Geschäftsräumen.

Die Postagenturmitarbeiter sind nach dem Postagenturvertrag auf das Post-, Bank- und Fernmeldegeheimnis

besonders verpflichtet. Die Vertraulichkeit über die ihnen bekanntgewordenen personenbezogenen Daten des Post- oder Postbankverkehrs müssen sie auch außerdienstlich und nach dem Ausscheiden aus der Postagentur wahren. Zum Teil wurden Mitarbeiter der früheren örtlichen Postfiliale von der neuen Postagentur übernommen. Die von der Deutschen Post AG für neue Mitarbeiter vorgenommene Einweisung am Arbeitsplatz in den ersten 14 Tagen bzw. in den folgenden vier Wochen erscheint bei dem umfangreichen Angebot an Post-, Postbank- und anderen neuen Dienstleistungen nur dann ausreichend zu sein, wenn die Mitarbeiter von den angebotenen weiteren Schulungsmaßnahmen und Workshops Gebrauch machen (können). Dies ist bei der knappen Personalausstattung einer Agentur, dem mit einer Schulungsmaßnahme verbundenen Personalausfall und den dadurch entstehenden Kosten nicht immer möglich. Ich habe der Post vorgeschlagen, daß die zuständige Post-Niederlassung, etwa bei der Einführung neuer Verkaufsprodukte und Verfahren oder im Rahmen einer (z. B. jährlichen) Inspektion der Agentur, ergänzende Schulungsmaßnahmen zum Erhalt eines hohen Qualitätsstandards des Personals vor Ort durchführen sollte. Ein hohes Qualitätsniveau des Personals, das bisher nur durch eine mehrjährige Laufbahnausbildung erreicht wurde, wird als wichtiger Wettbewerbsfaktor auch im Interesse der Deutschen Post AG liegen.

Der Gesamteindruck aus meinen Kontrollen ist gut. Das paßt dazu, daß in den mir zugegangenen Zuschriften zwar allgemein Probleme und Risiken, aber keine konkreten Verstöße gegen das Postgeheimnis dargelegt wurden.

29.5 Postdienstleistungen und Werbung

Die Deutsche Post AG ist nach der Umstrukturierung von einer Behörde zu einem privatwirtschaftlichen Unternehmen nicht mehr nur in ihrem klassischen Geschäftsfeld, der Erbringung von Postdienstleistungen, tätig, sondern hat inzwischen neue Geschäftsfelder erschlossen, die häufig in einem Zusammenhang mit einer bestimmten Postdienstleistung stehen. Da der Anteil von adressierten Werbesendungen am Beförderungsaufkommen permanent zugenommen hat, ist es nachvollziehbar, daß die Post auch selbst im Direktmarketing tätig wird und so zugleich diese Sendungsformen fördert.

29.5.1 Adressenwaschen durch Beteiligung mehrerer Unternehmen

Ein Bürger, der keine Direktwerbung erhalten möchte und sich darum bemüht, daß seine Anschrift dafür nicht genutzt wird, erhielt gleichwohl eine an ihn adressierte Werbesendung. Um die Ursache zu klären und Wiederholungen zu vermeiden, hat er sich zunächst an das Unternehmen gewandt, für dessen Leistung geworben und das auch als Absender der Werbung angegeben wurde.

Das werbende Unternehmen, der Betreiber eines Freizeitparks, erläuterte dem hilfesuchenden Bürger, daß es sich wegen der Werbemaßnahme an ein Direktmarketing Center der Deutschen Post AG gewandt habe, das sowohl mit der Erbringung der Postdienstleistungen als auch mit der Vermittlung einer geeigneten Agentur für die Erstellung des Werbematerials und die Auswahl der Zielgruppe des Werbeschreibens (mailing) beauftragt worden sei. Das Direktmarketing Center betreut Interessenten und Kunden (= werbende Unternehmen) so, daß diese möglichst erfolgreich die Dienste der Post AG für den Transport und die Zustellung von sog. mailings nutzen können.

Die vom Betreiber des Freizeitparks über die Deutsche Post AG beauftragte Agentur hatte – wie die meisten der in diesem Markt tätigen Agenturen – keine oder keine ausreichenden Adressbestände und wandte sich deshalb an einen Adressenhändler. Der Adressenhändler nutzt außer seinen eigenen Adressen, die er auf eigene Rechnung vermietet, auch fremde Adressen von Unternehmen, die diese Adressen zur Erfüllung eigener Geschäftszwecke gespeichert haben und auch – gegen Entgelt – auf Vermittlung des Adressenhändlers von anderen zu Werbezwecken nutzen lassen (vermieten). Auch im vorliegenden Fall hat eine Firma, die in ihrem Bestand auch die Anschrift des betroffenen Bürgers führte, diese über einen Adressenhändler zu Werbezwecken nutzen lassen.

Der betroffene Bürger erfuhr das alles nur langsam. Denn zunächst berief sich das Direktmarketing Center auf sein Geschäftsgeheimnis und wollte deshalb seine Partner bei dieser Aktion nicht benennen. Dazu war es nach dem Wortlaut des BDSG auch nicht verpflichtet, denn der datenschutzrechtliche Auskunftsanspruch des Betroffenen gilt nur gegenüber den Stellen, die Daten zu seiner Person speichern, und das Direktmarketing Center hatte die Anschrift nicht gespeichert, sondern deren Nutzung vermittelt. So bedurfte es einiger hartnäckiger Bemühungen, bei denen ich den Betroffenen unterstützen konnte, bis ihm die Zusammenhänge offengelegt wurden.

Auch wenn die Angelegenheit damit zu einem erträglichen Ende kam, hat auch dieser Fall gezeigt, daß bei der anstehenden Novellierung des BDSG die Rechtssituation der Betroffenen verbessert werden sollte (s. auch Nr. 2.1.2).

29.5.2 Unerwünschte Werbung für postphilatelistische Produkte

Häufig fragen mich Bürger, die niemals bei der Post Sondermarken, Ersttagsbriefe oder andere postphilatelistische Produkte bestellt hatten und trotzdem von der Postphilatelie, einem Geschäftsfeld der Deutschen Post AG, unerwünschte Werbezuschriften erhielten, aus welcher Quelle die Post ihre Anschrift habe. Aber auch ehemalige Kunden, die der Post bereits mitgeteilt hatten, daß sie künftig keine Postphilateliewerbung mehr wünschten, beschwerten sich bei mir über weitere Werbezuschriften. In einigen Einzelfällen hatte die Deutsche Post AG auch nach mehrmaliger Aufforderung, die Daten aus den für Werbezwecke genutzten Adressbeständen zu löschen, die Zusendung unerwünschter Werbung immer noch nicht eingestellt. Die Ursachen dieser Probleme waren die Undurchsichtigkeit des Verfahrens im Direktmarketing, Ungenauigkeiten bei Adressangaben und auch einige Pannen.

Grundsätzlich werden diese mailings im Auftrag der Deutschen Post AG von einem beauftragten Dienstleistungsunternehmen erstellt. Dieses verwendet für die einzelnen Werbesendungen in unterschiedlicher Zusammensetzung neben eigenen Adressen von Personen, die sich bereits für die Postphilatelie interessiert haben, auch Adressen eines Adressenhändlers, der sie nach bestimmten Kriterien teils aus seinem Bestand und teils aus weiteren Quellen ausgewählt hat. Aus welcher Quelle eine Adresse im Einzelfall stammt, kann das Dienstleistungsunternehmen nur anhand der auf der Sendung angebrachten Unterscheidungsnummer feststellen. Ohne deren Kenntnis kann die Post einem anfragenden Bürger keine Auskunft über die Herkunft seiner Adresse geben, und löschen kann sie seine Daten nur aus ihrer eigenen Adressdatei.

Die Deutsche Post AG läßt seit einiger Zeit die zur Postphilatelie verlangten Auskünfte nach § 19 BDSG in ihrem Auftrag durch das beauftragte Dienstleistungsunternehmen erteilen, da nur der Dienstleister in der Lage sei, eine korrekte Auskunft zu erteilen. Sie will jedoch künftig diese Aufgabe unter Zuhilfenahme des Dienstleistungsunternehmens übernehmen.

Der Dienstleister erhält auch die Anträge auf Löschung von Adressdaten. Die Post AG räumt ein, daß es in der Vergangenheit dabei zeitliche Verzögerungen von 4 bis 8 Wochen bis zur tatsächlichen Löschung der Adressen aus den genutzten Datenbeständen gegeben hat, so daß aus diesem Grunde in Einzelfällen noch Werbezuschriften an ehemalige Kunden oder andere Personen gelangt sind.

Um für die Zukunft bei Personen, die keine Werbung für Postphilatelie-Produkte wünschen, mit größtmöglicher Zuverlässigkeit solche Zusendungen zu vermeiden, hat die Deutsche Post AG nach dem Vorbild der Robinson-Liste des Deutschen Direktmarketing Verbandes eine spezielle „Postphilatelie-Robinsonliste“ für deren Anschriften angelegt. Die Post behandelt die Anträge auf Löschung der Daten so, daß die Anschriften nicht nur im Bestand gelöscht, sondern zugleich in die Datei der „Postphilatelie-Robinsonliste“ aufgenommen werden, damit sie zum Datenabgleich mit anderen Datenbeständen und damit zur Vermeidung von unerwünschter Werbung zur Verfügung stehen. Ich habe gegen die Speicherung der Adressdaten von Werbeverweigerern in der „Postphilatelie-Robinsonliste“ keine Bedenken, da die Deutsche Post AG nur so dem Wunsch der Personen, die keine Werbung wünschen, Rechnung tragen kann.

In einigen Fällen hat auch die unterschiedliche Schreibweise von Namen und Adressen zu unerwünschter Werbung trotz Widerspruchs geführt. Wenn z. B. die Anschrift von **Michel Mustermann in Musterstadt** als Adresse registriert ist, an die keine Werbung geschickt werden soll, kann es durchaus sein, daß in einem anderen Adressbestand die Adresse **M. Mustermann in Musterstadt** vorhanden ist und wegen der unterschiedlichen Schreibweise nicht ausgesondert wird. Die Deutsche Post AG hat mir zugesichert, daß in Zukunft durch eine „weichere Adressprüfung“ bei solchen geringfügigen Abweichungen Personenidentität angenommen und damit das „Durchrutschen“ solcher Adressen vermieden wird. Es kann auch damit aber nicht absolut ausgeschlossen werden, daß über die Anmietung eines neuen Adressbestandes durch den beauftragten Dienstleister erneut eine Anschrift für ein Postphilatelie-mailing genutzt wird, die in der Postphilatelie-Robinsonliste als Werbeverweigereranschrift – in etwas anderer Schreibweise – bereits vorhanden ist.

29.6 Zweite Postkartenaktion

Nachdem die Deutsche Post AG im Herbst 1996 einen – mißglückten – Versuch unternommen hatte, die aktuellen Anschriften der in den ca. 36,5 Millionen Haushalten in Deutschland lebenden Personen zu erhalten, hat sie mein Beratungsangebot für eine zweite, datenschutzrechtlich unbedenkliche **Adressenerhebung** angenommen (vgl. 16. TB Nr. 29.4). Die daraufhin im Frühjahr 1997 durchgeführte zweite Auskunftskartenaktion hat aufgrund der sorgfältigen Vorbereitung zu keinen nennenswerten Beschwerden und zu einer insgesamt positiven Resonanz geführt. Denn auf den Vordrucken war klar darauf hingewiesen, daß die Betroffenen selbst darüber entscheiden können, ob sie ihre Anschrift angeben oder nicht.

Zum Jahresende 1998 ist die Deutsche Post AG erneut mit einem Beratungswunsch zur Anschriftenprüfung an mich herangetreten. Im Frühjahr 1999 will die Post diese Adressen und andere, die häufig zur Versendung insbesondere von adressierter Werbung genutzt werden, daraufhin überprüfen, ob sie – noch – korrekt sind. Mit der Post AG ist abgesprochen, daß dabei keine neuen Anschriften aufgenommen werden. Ferner soll diese Aktion der Öffentlichkeit rechtzeitig vorher angekündigt und erläutert werden. Ich begrüße die von der Post AG vorgesehene frühzeitige Information der Bürgerinnen und Bürger sehr, trägt sie doch mit dazu bei, Mißtrauen gegenüber den Postzustellern, die diese Verifizierung durchführen sollen, von vorneherein zu vermeiden.

29.7 Die Gebäudedatei – oder wie man durch irreführende Werbung ein datenschutzrechtliches Problem schafft

Für erhebliche Aufregung und zahlreiche Eingaben und Anrufe sorgte Anfang September 1998 ein Artikel der Deutschen Post AG in ihrer Kundenzeitschrift „Postplus“. Zur Nutzung für Direktwerbung offerierte die Post darin eine **posteigene Gebäudedatei** mit Angaben über etwa 16 Millionen Gebäude, spezifiziert nach neun Kriterien wie Ein- oder Zweifamilienhaus, Alt- oder Neubau, mit oder ohne Garten, Garage etc., und aktualisiert durch die Postzusteller, die auf ihren Zustellgängen dafür angeblich Informationen sammeln. Die Reaktionen in der Öffentlichkeit auf die Berichte darüber waren empört, und viele Bürger fragten, wem man überhaupt noch vertrauen könne, wenn sogar schon die Briefträger die Wohnverhältnisse ausspionierten. Zum Glück waren diese Angaben der Deutschen Post AG in der Kundenzeitschrift weitgehend **irreführend bzw. falsch** und entsprachen in den Kernaussagen nicht den Tatsachen.

So handelt es sich bei der dort genannten Gebäudedatei, anders als behauptet, um die Datenbank eines großen deutschen Direktmarketing-Dienstleisters, die von der Post AG für ihr Produkt „Postwurf Spezial" genutzt wird.

Die Daten werden auch nicht *„aufgrund der Fakten, die die Zustellerinnen und Zusteller auf ihren Zustellgängen sammeln, regelmäßig aktualisiert"*, sondern die Pflege der Daten erfolgt durch den Dienstleister. Die Deutsche Post AG stellt diesem hierfür weder Informationen der Zustellerinnen und Zusteller zur Verfügung, noch duldet sie eine entsprechende Nebentätigkeit. Allein die Anzahl der Abgabestellen je Haus unter Berücksichtigung der Anzahl der Werbeverweigerer wird von der Post beigesteuert. Damit kann dann die richtige Anzahl von Werbebroschüren je Haus mit Straße und Hausnummer – aber ohne Namen – teiladressiert und denjenigen zugestellt werden, die sich Werbung nicht durch einen entsprechenden Aufkleber am Briefkasten verbeten haben.

Im Gegensatz zu den Ausführungen der Post in dem genannten Artikel, *„die Daten über das Wohnhaus können mit soziodemographischen und statistischen Daten kombiniert werden, z. B. mit Alter, Kaufkraft und Konsumschwerpunkte der Hausbewohner"*, können diese Merkmale nicht individuell auf einzelne Hausbewohner bezogen werden. Bei diesen soziodemographischen Daten handelt sich lediglich um Angaben über Schätzungen oder begründete Erwartungen, z. B. von Alter oder Kaufkraft. Sie werden auch nicht vom Postdienst erhoben, sondern von dem Dienstleister.

Hätten die Angaben in der Postkundenzeitschrift „Postplus" den Tatsachen entsprochen, so wäre diese Datenverarbeitung offensichtlich rechtswidrig gewesen und von mir beanstandet worden. Meine datenschutzrechtliche Bewertung eines Sachverhalts orientiert sich aber an den Fakten und tatsächlichen Verfahrensabläufen und nicht an den irreführenden oder falschen Aussagen in einer Kundenzeitschrift, auch wenn sich ein Unternehmen hierdurch selbst in den Verdacht des Bruchs des Postgeheimnisses und der Verletzung datenschutzrechtlicher Vorschriften bringt.

So war nach einer detaillierten Prüfung des Sachverhalts und der tatsächlichen Abläufe bei der Nutzung der Gebäudedatei durch die Post nur festzustellen, daß die Auswahl von Teiladressen ohne Namen und die Bereitstellung der Zahlen über die Abgabestellen je Haus durch die Deutsche Post AG zur genauen Ermittlung der Anzahl von teiladressierten Werbesendungen nicht gegen datenschutzrechtliche Vorschriften verstoßen.

Auf Grund der breiten öffentlichen Diskussion und der zahlreichen Beschwerden von Bürgern habe ich die Post aufgefordert, ihre Aussagen in der Kundenzeitschrift „Postplus" zu korrigieren und insbesondere die Trennlinie zwischen dem Geschäftsfeld „Postdienstleistung", das wegen der besonderen Sensibilität der Daten speziellen straf- und datenschutzrechtlichen Vorschriften unterliegt, und den anderen Aktivitäten in geeigneter Weise der Öffentlichkeit transparent zu machen. Eine Klarstellung ist dann auch in der November-Ausgabe von 1998 der Kundenzeitschrift „Postplus" erfolgt.

Der durch die eigenen irreführenden Angaben verschuldete Vertrauensverlust wird nicht so leicht auszugleichen sein. Er hätte mit hoher Wahrscheinlichkeit vermieden werden können, wenn den Beteiligten die Bedeutung des Datenschutzes für die traditionell vertrauensbedürftige Arbeit der Post bewußt gewesen wäre. Damit hat dieser wie auch ein anderer Fall (s. Nr. 29.8) Defizite bei der Einbindung des Datenschutzes in die Unternehmensabläufe der Deutschen Post AG offenbart, die nicht zuletzt im Interesse des Unternehmens selbst umgehend behoben werden müssen.

29.8 Post-„Mutter" half ihrer Tochter – und verletzte dabei datenschutzrechtliche Vorschriften

Der Rauch über den Ärger mit der Gebäudedatei (s. Nr. 29.7) hatte sich eben verzogen, als sich bereits neues datenschutzrechtliches Unheil für die Deutsche Post AG ankündigte. Gerade als die Deutsche Post AG mein Beratungsangebot in Datenschutzfragen für eine geplante Kundenakquisition im Frachtpostbereich nutzte, wobei Einigkeit über den datenschutzrechtlich möglichen Rahmen erreicht wurde, ereigneten sich im Raum Wuppertal/Neuss/Düsseldorf genau die Verletzungen datenschutzrechtlicher Vorschriften, vor denen ich die Post im Rahmen meiner Beratungsaufgabe bei der Kundenakquisition im Frachtpostbereich gerade bewahrt hatte. Der Fall zeigt leider auch, wie gering der Stellenwert des Datenschutzes in einem Wirtschaftsunternehmen gelegentlich geschätzt wird. Der Sachverhalt wurde bekannt, weil ein Konkurrenzunternehmen der Deutschen Post AG auf den Vorgang aufmerksam gemacht wurde.

Zwei Beschäftigte der Regionalniederlassung Düsseldorf eines Post-Tochterunternehmens hatten im August 1998 mehrere Postfachanlagen der Deutschen Post AG aufgesucht bzw. die Filialen angeschrieben und gebeten, die Post-Tochter bei der Wettbewerbsbeobachtung zu unterstützen. Dazu sollten Mitarbeiter der Deutschen Post AG den Posteingang der Postfachinhaber auf Sendungen von Konkurrenzunternehmen der Post-Tochter durchsehen. Von solchen Sendungen sollten sie den Absender sowie Namen, Anschrift und Telefonnummer des Empfängers in einer Liste erfassen und diese an die Post-Tochter schicken. Dies ist nach meinen Feststellungen auch so geschehen.

Die Aktion wurde Ende August 1998 begonnen und am 25. September 1998 auf Grund eigener datenschutzrechtlicher Bedenken nur im Bereich der Niederlassung Wuppertal eingestellt; in den Postfilialen mit Postfachanlagen im Raum Neuss und Düsseldorf sind diese Aufzeichnungen noch bis Anfang Oktober 1998 vorgenommen und erst nach Bekanntwerden des Antrags auf Erlaß einer einstweiligen Verfügung eingestellt worden. Der Antrag hatte Erfolg.

Schon das Durchsehen der nur zur Beförderung anvertrauten Briefe sowie das Festhalten der o.a. Daten in den dafür vorgesehenen Listen waren als unbefugtes Nutzen bzw. Speichern von Daten über Teilnehmer am Postverkehr unzulässig, weil die Postdienstunternehmen-Daten-

schutzverordnung (PDSV) dafür keine Erlaubnis enthält. Die Übermittlung dieser Daten wäre ebenso wie ihre eventuelle Bekanntgabe an einen anderen Mitarbeiter der Deutschen Post AG nach § 206 StGB (Verletzung des Postgeheimnisses) strafbar gewesen. Es ist bedauerlich, daß diese Aktion trotz der offensichtlichen Rechtswidrigkeit vier Wochen lang von Mitarbeitern der Deutschen Post AG durchgeführt wurde. Und es ist die Folge eines Organisationsmangels bei der Deutschen Post AG, daß deren Mitarbeiter Aufträge eines Tochterunternehmens ausführen, ohne daß zuvor auch nur eine wenigstens pauschale Prüfung der Zulässigkeit des verlangten Umgangs mit zu schützenden Daten erfolgte, die zweifellos die Rechtswidrigkeit des beabsichtigten Vorgehens hätte erkennen lassen. Ich habe das **beanstandet** (s. Anlage 3).

In ihrer Stellungnahme hat mit die Deutsche Post AG mitgeteilt, daß durch organisatorische und personelle Maßnahmen sichergestellt wird, daß sich derartige Verstöße zukünftig nicht wiederholen. Darüber hinaus soll der Datenschutz in diesem besonders schützenswerten Bereich gestärkt werden.

30 Statistik

30.1 Volkszählung 2001

Bei der von der EU für das Jahr 2001 vorgeschlagenen Volkszählung (VZ) wird es einen Methodenwechsel von der vollständigen Befragung aller Einwohner (nach dem Vorbild früherer VZ) zu einer hauptsächlich registergestützten Datengewinnung geben. Das bedeutet, daß der größte Teil der benötigten Daten aus bestehenden Verwaltungsregistern entnommen und um eine repräsentative Stichprobenerhebung ergänzt werden soll. Dieser Methodenwechsel, der durch das sog. Volkszählungsurteil des Bundesverfassungsgerichtes von 1983 angestoßen und von Bundestag und Bundesregierung unterstützt wird (s. **Anlage 4**), hat erhebliche Konsequenzen für das System der Statistik in Deutschland:

Es müssen die rechtlichen und organisatorischen Voraussetzungen geschaffen werden, die eine Nutzung der Verwaltungsdateien für einen Zensus ermöglichen.

Zunächst ist zu prüfen, wie vollständig und zuverlässig die Volkszählungsergebnisse aus den Verwaltungsdateien – insbesondere aus den Melderegistern – gewonnen werden können. Für die erkannten Defizite muß dann geklärt werden, ob deren Auswirkungen auf die Ergebnisse tolerierbar sind oder ob und welche Maßnahmen noch zu treffen sind, sei es zur Verbesserung der Verwaltungsdateien, sei es zur Ergänzung der Registerauswertung durch stichprobenweise Befragungen der Bürger.

Die Statistiker von Bund und Ländern haben für die VZ zwei Modelle, ein Bundesmodell und ein Ländermodell, entwickelt.

30.1.1 Das Bundesmodell

Das **Bundesmodell** konzentriert sich auf den bevölkerungsstatistischen Kern des Zensus. Damit werden die amtlichen Einwohnerzahlen für Bund, Länder und Gemeinden festgestellt, die Grundlage für den horizontalen und vertikalen Finanzausgleich und für die Bevölkerungsfortschreibung sind. Außerdem gewinnt man damit kleinräumige demographische Strukturdaten als Basis für statistische Auswahlpläne. Diese Ergebnisse sollen aus den Melderegistern entwickelt werden.

Daneben werden in einem erwerbsstatistischen Teil Daten über abhängig Beschäftigte, über das Pendlerverhalten sowie über Arbeitslose aus den Registern der Bundesanstalt für Arbeit aufbereitet.

Die Registerauswertungen werden ergänzt um Stichprobenerhebungen bei 1% der Einwohner, um – repräsentativ – Angaben zur Ausbildung, zu den Wohnverhältnissen und zur Erwerbstätigkeit von Selbständigen, mithelfenden Familienangehörigen und geringfügig Beschäftigten zu erfragen.

Das Bundesmodell stellt somit Ergebnisse aus verschiedenen Quellen zusammen (s. Abb. 10), nimmt aber keine Verknüpfungen zwischen den personenbezogenen Daten der einzelnen Teile vor.

30.1.2 Das Ländermodell

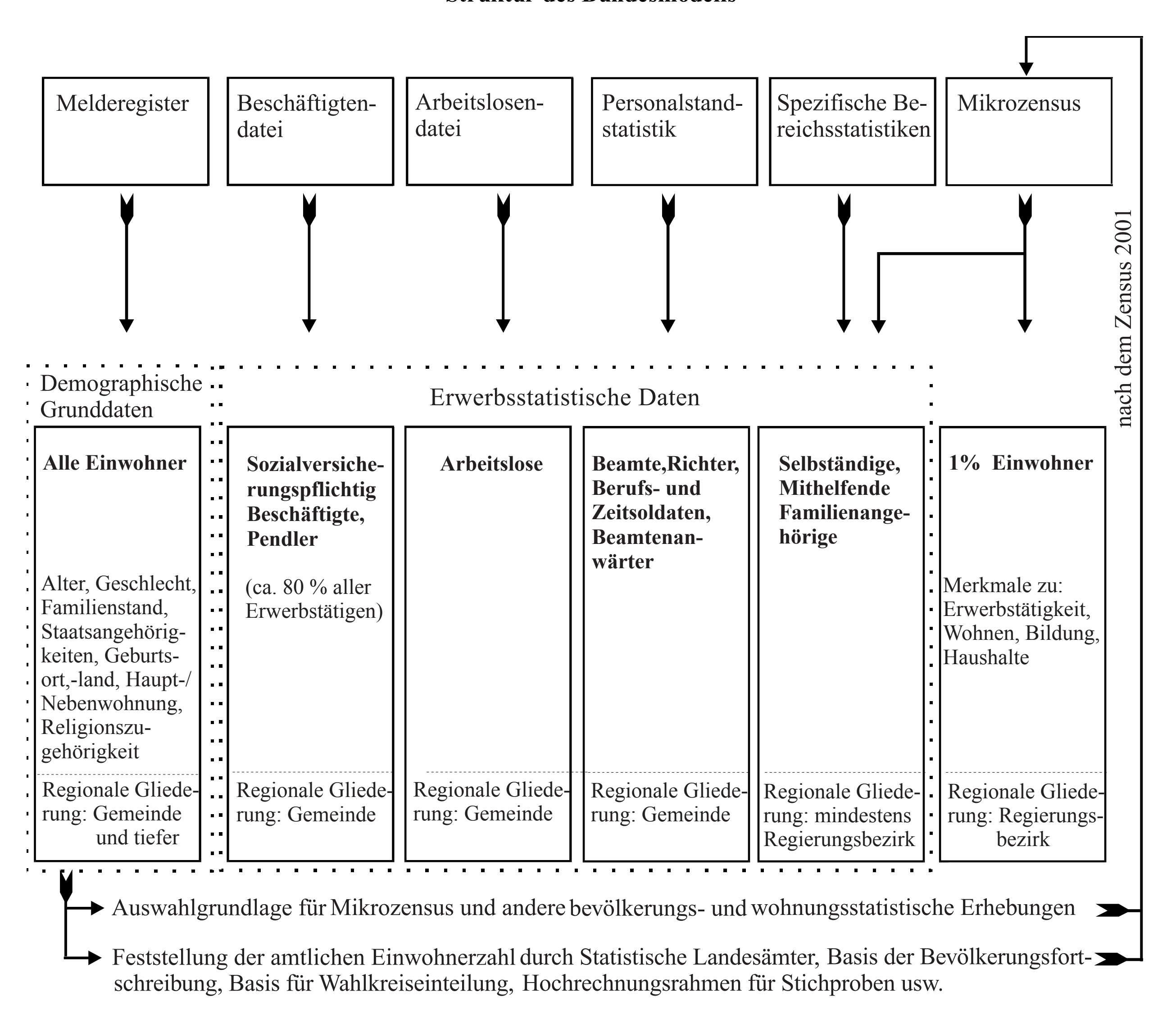
Das **Ländermodell** will dem weitergehenden Informationsbedarf von Ländern und Gemeinden mit der Erweiterung des Bundesmodells um eine primärstatistische Vollerhebung – in Form einer postalischen Befragung aller Gebäudeeigentümer – Rechnung tragen. Im Gegensatz zum Bundesmodell sollen darüber hinaus alle Daten personenbezogen zur VZ-Datei zusammengeführt werden, so daß zu jeder Person ein Gesamt-Datensatz entsteht. Dieser Datensatz entspricht inhaltlich etwa dem, der bei früheren VZ durch direkte Befragung gewonnen wurde.

Das Ländermodell setzt sich aus einem Grundmodul und einem Ergänzungsmodul zusammen (s. Abb. 11). Es sieht die Verknüpfung von Einzeldaten aus bestehenden Registern (Melderegister, Dateien der Bundesanstalt für Arbeit) mit Einzeldatensätzen aus ergänzenden Erhebungen (Gebäude- und Wohnungszählung sowie postalische Ergänzungsstichprobe im Erwerbsbereich) vor. Die verschiedenen Datenquellen sollen gegeneinander auf Plausibilitäten geprüft werden, um eine hohe Qualität der Registerauswertungen zu erreichen.

Andere Staaten – wie beispielsweise in Skandinavien – verfahren nach diesem Modell. Dort wird allerdings die Verknüpfung amtlicher Dateien über ein eindeutiges Personenkennzeichen (PK) sichergestellt. Ohne dieses in Deutschland nicht eingeführte PK würde die Verknüpfung zu vermehrten Rückfragen bei den beteiligten Stellen und beim Bürger führen; und zwar nicht nur deshalb, weil die Daten tatsächlich falsch sind, sondern weil die ausgewerteten Register beispielsweise unterschiedliche Schreibweisen von Namen und Vornamen enthalten und deshalb nicht zum gleichen Datensatz zusammengefaßt werden können.

Abbildung 10 (zu Nr. 30.1.1)

Struktur des Bundesmodells



Unstimmigkeiten treten ferner bei großen Mietwohnanlagen auf, wenn die von Gebäudeeigentümern gemachten Angaben zum Wohnungsinhaber und zur Zahl der Personen in der Wohnung ungenau sind und dann mit den Meldedaten nicht übereinstimmen.

Die Verknüpfung verschiedener, wegen ihrer unterschiedlichen Zwecke oft nicht kompatibler Datenbestände wird zahlreiche Rückfragen und Überprüfungen nach sich ziehen. Die dabei auftretende intensive Beschäftigung mit den Verhältnissen einzelner Bürger birgt aus meiner Sicht Datenschutzrisiken. Bisher liegen keine Ausarbeitungen vor, wie diese Kontrollvorgänge ablaufen sollen.

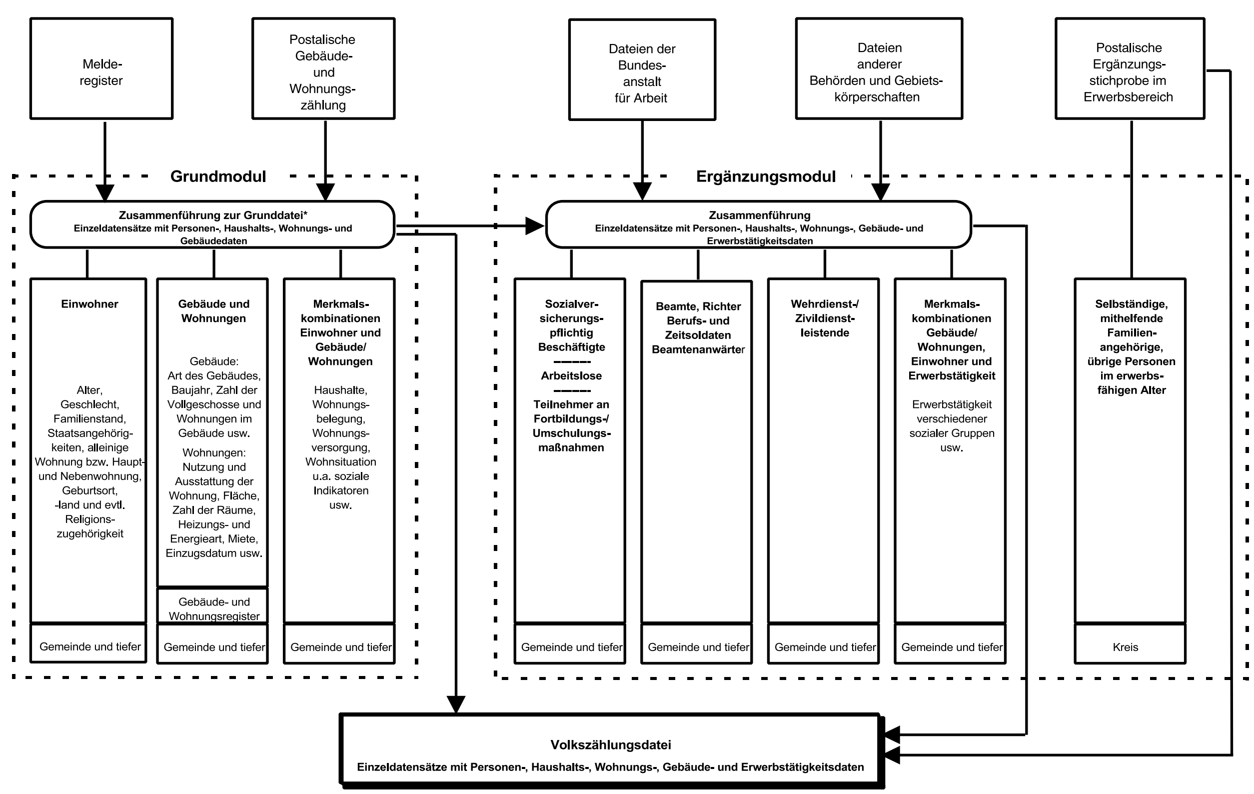
30.1.3 Maßnahmen zur Verbesserung der Melderegister

Die Qualität der Melderegister ist für die Qualität der Volkszählungsergebnisse von ausschlaggebender Bedeutung, da sie bei einem registergestützten Zensus die Grunddaten liefern sollen. Daher wurde eine Arbeitsgruppe der Innenministerkonferenz beauftragt, die Qualität dieser Register zu untersuchen und bei Bedarf Vorschläge zu ihrer Verbesserung zu entwickeln.

Da die administrativen Maßnahmen – nach Auffassung der Verwaltung – den gesetzlichen Rahmen bereits weitgehend ausgeschöpfen, wurden Anfang 1999 im BMI Vorschläge für bundeseinheitliche Rahmenbedingungen zur Verbesserung der Richtigkeit und Vollständigkeit der Melderegister entwickelt. Wesentlich darin ist zum einen eine Befugnisnorm für die Meldebehörden zur Überprüfung solcher Meldedaten, bei denen wahrscheinlich ist, daß sie zwischenzeitlich unrichtig geworden sind, wie z. B. Daten über Nebenwohnungen oder über jüngere Einwohner, die mit hoher Wahrscheinlichkeit mobil sind. Zum anderen sollen öffentliche Stellen, denen Meldedaten für die Erfüllung ihrer Aufgaben übermittelt werden, ihrerseits Unstimmigkeiten den Meldebehörden mitteilen. Schutzwürdige Belange sind dabei zu berück-

Abbildung 11 (zu Nr. 30.1.2)

Struktur des Ländermodells



* Auswahlgrundlage für den Mikrozensus und andere bevölkerungs- und wohnungsstatistische Erhebungen, Feststellung der **amtlichen Einwohnerzahl** durch die Statistischen Landesämter, Basis der Bevölkerungsfortschreibung und der Fortschreibung des Gebäude- und Wohnungsbestandes, Hochrechnungsrahmen für Stichproben.

sichtigen und es dürfen nur solche Daten übermittelt werden, die für die Führung des Melderegisters erforderlich sind.

Weil an korrekten Meldedaten ein allgemeines, weit über die registergestützte VZ hinausreichendes Interesse besteht, habe ich gegen die Erweiterung des Melderechts keine grundsätzlichen Einwendungen.

30.1.4 Vorbereitung der VZ

Bisher liegen keine Erfahrungen mit einer registergestützen VZ vor. Daher müssen die neuen Verfahren zur Datengewinnung vor der Einführung getestet werden. Mit den vorgesehenen Untersuchungen soll insbesondere geprüft werden, ob die von den Meldebehörden übermittelten Daten vollständig, richtig und aktuell sind.

Nach dem Stand eines Gesetzentwurfs (bei Redaktionsschluß) ist beabsichtigt,

- die Berichtswege von den Meldebehörden sowie der von ihnen beauftragten überörtlichen Rechenzentren zu den statistischen Ämtern zu erproben,
- zu klären, ob alle benötigten Hilfsmerkmale aus den Registern der Meldebehörden bereitgestellt werden können,
- festzustellen, in welchen Datenformaten die Merkmale übermittelt werden und wie sie in einen bundeseinheitlichen Statistikdatensatz umzusetzen sind und
- die Verfahren zur Plausibilitätsprüfung zu testen.

Die Probeerhebung bei den Meldebehörden soll sich auf etwa 0,9% der Bevölkerung erstrecken und Angaben zu 8 Erhebungsmerkmalen und einer Reihe von Hilfsmerkmalen umfassen, die Eindeutigkeits- und Plausibilitätsprüfungen dienen. Die Daten dürfen nur für die Vorbereitungsarbeiten genutzt werden und sind spätestens am 31. Dezember 2001 zu löschen. Davon ausgenommen ist eine Datei mit den verschiedenen Schreibweisen von Ortsnamen, die bis zum Abschluß der VZ bestehen bleibt.

An den Beratungen zum Gesetzentwurf war ich beteiligt. Die Probeerhebung begegnet keinen datenschutzrechtlichen Bedenken.

Am Rande meiner Beratungen habe ich nachdrücklich angeregt, von einer Geldbuße wegen unterlassener Meldepflichten abzusehen, wenn Bürger aus Anlaß ihrer Befragung wegen unklarer Registerauskünfte von sich aus ihre Meldedaten korrigieren lassen. Diese Möglichkeit sollte ihnen eröffnet und anhand eines Informationsblattes erläutert werden.

30.2 Statistikregistergesetz

Das Gesetz zum Aufbau eines Unternehmensregisters für statistische Verwendungszwecke (vgl. 16. TB Nr. 30.3) ist am 24. Juni 1998 in Kraft getreten. Mit der Umsetzung der Verordnung der EU Nr. 2186/93 vom 22. Juli 1993 ist damit die rechtliche Grundlage für die Übermittlung von Informationen aus Wirtschaft und Verwaltung an die statistischen Ämter, für die Geheimhaltung dieser Daten sowie für die Nutzungsmöglichkeiten des Registers geschaffen.

Dieses Unternehmensregister wird zwar beim Statistischen Bundesamt geführt, es ist jedoch selbst keine Statistik, sondern eine Datei, die für unterschiedliche – und auch künftig erst festzulegende – Verwendungen angelegt und laufend gepflegt wird. Damit können wichtige Informationen über die Struktur der Unternehmen innerhalb der EG bereitgestellt werden, insbesondere zur Beobachtung struktureller Veränderungen der Wirtschaft, die auf Maßnahmen wie Vereinigung, Teilhaberschaft, Aufkauf, Fusion oder Übernahme zurückzuführen sind.

Das Register soll auch für nationale Statistiken genutzt werden, z. B. um die für eine Statistik zu befragenden Unternehmen auszuwählen. Darüber hinaus dürfen die statistischen Ämter bestimmte Angaben als Erhebungsmerkmale für Wirtschafts- und Umweltstatistiken verwenden, um die Unternehmen von Auskünften hierüber zu entlasten.

Die datenschutzrechtlichen Regelungen für Aufbau, Pflege und Nutzung des Registers sind angemessen. Dem damaligen Vorschlag, ein einheitliches Unternehmenskennzeichen einzuführen, ist der Gesetzgeber nicht gefolgt. Gegen dieses Kennzeichen sprach nicht nur der erhebliche Aufwand für seine Einführung. Mit diesem Verzicht wurde auch meinen Bedenken Rechnung getragen, daß es zu einem Personenkennzeichen für Selbständige werden könnte, wenn es – wie zu erwarten – auch außerhalb der Statistik als Ordnungsmerkmal verwendet würde.

30.3 Zugangsrecht der Statistik zu allen Verwaltungsdaten?

30.3.1 Statistik im schlanken Staat

Die politische Forderung nach Verschlankung staatlicher Verwaltung zur Steigerung deren Wirtschaftlichkeit wird von der Statistik aufgegriffen, um über ein allgemeines Zugangsrecht zu Verwaltungsdaten statistische Erhebungen zu erleichtern. In den „Empfehlungen des Statistischen Beirates zur Bundesstatistik für die 14. Wahlperiode des Deutschen Bundestages“ wird diese schon früher erhobene Forderung nach stärkerer Nutzung von Verwaltungsunterlagen für statistische Zwecke wiederholt (vgl. auch 16. TB Nr. 30.1). Schon heute werden Verwaltungsdaten für statistische Zwecke genutzt. Durch ein verstärktes Heranziehen dieser Daten für alle Statistikbereiche könnten – so der Beirat – die statistischen Arbeiten rationalisiert und die statistischen Berichtslasten der Wirtschaft minimiert werden. Um die in Verwaltungsregistern enthaltenen Daten für Zwecke der Bundesstatistik nutzbar zu machen, sollte der amtlichen Statistik ein allgemeines Zugangsrecht eingeräumt werden. Darüber hinaus müßte unter Beachtung der qualitativen Anforderungen an die Bundesstatistik ein „statistiktauglicher“ Aufbau der in Frage kommenden Register sichergestellt werden.

30.3.2 Ergebnisse eines Gutachtens

Um die fachlichen und rechtlichen Möglichkeiten und Voraussetzungen für Wirtschafts- und Umweltstatistiken aufzuzeigen, hat das BMWi 1997 ein Gutachten in Auftrag gegeben. Der Entwurf des Schlußberichts wurde mir im September 1998 vom BMWi zur Verfügung gestellt. Danach eignen sich im wesentlichen nur zwei bis drei der untersuchten Verwaltungsregister für die Statistik. Selbst bei diesen müßten noch z. T. umfangreiche Änderungen technischer, organisatorischer und auch inhaltlicher Art vorgenommen werden, damit sie für die Statistik verwendbar sind. Das würde für die Verwaltung bedeuten, daß sie in allen Phasen ihrer Datenverarbeitung die Belange der Statistik berücksichtigen müßte, angefangen von der Erhebung ggfs. zusätzlicher Angaben, der Erhebung mit anderen Vordrucken, Formaten und Terminen, über die Nutzung, die nun zwischen statistischen und verwaltungsmäßigen Daten zu unterscheiden hat, bis hin zu unterschiedlicher Speicherungsdauer und abweichenden Löschungsfristen.

Unter diesen Umständen dürfte es schwierig werden, das Statistikgeheimnis zu wahren.

Zweifelhaft dürften auch die anvisierten Rationalisierungserfolge sein. Einsparungen ergeben sich nur dort, wo Unternehmen bisher dieselben Daten sowohl der Verwaltung als auch der Statistik liefern müssen. Dieser Fall ist jedoch höchst selten, wie die Untersuchung ergeben hat.

30.3.3 Probleme des Statistikrechts

Änderungen im Verwaltungsverfahren, insbesondere die Erhebung und Weiterverarbeitung von Daten zu ausschließlich statistischen Zwecken, sind mit dem geltenden Recht nicht vereinbar. Die Verwaltung ist mit dem Erforderlichkeitsgebot daran gebunden, daß sie nur über die Daten verfügen darf, die sie für die Erfüllung ihrer Aufgaben benötigt. Zahlreiche Gesetze für besonders geschütze Bereiche – wie der Sozial- und Finanzbereich – enthalten abschließende Regelungen zum Speicherungsumfang und den Übermittlungsmöglichkeiten und lassen somit keine weitergehende Datenverarbeitung zu. Auch § 9 BStatG verlangt für jede Statistik neben der Bestimmung der Erhebungsmerkmale die Festlegung der Art der Erhebung, des Berichtszeitraums und -zeitpunkts, der Periodizität und des Kreises der zu Befragenden. Ohne rechtliche Änderungen ist daher der Statistik der Zugang zu Verwaltungsdaten nicht zu ermöglichen.

Eine pauschale gesetzliche Regelung, nach der die Statistik nicht nur einen generellen Zugang bekommt, sondern nach der sie auch bestimmen kann, welche Daten von der Verwaltung verarbeitet und übermittelt werden,

halte ich weder für zweckmäßig, noch angesichts der möglichen Folgen für erstrebenswert. Gegen ein allgemeines Zugangsrecht spricht,

– daß nur ganz wenige Verwaltungsdateien statistiktauglich sind;

– daß die Frage, wer wann welche Daten liefern soll, dann nicht mehr im Gesetzgebungsverfahren diskutiert wird;

– und daß die Transparenz beim Betroffenen Einbußen erleidet, weil seine Mitwirkung am Datenverkehr nicht mehr gebraucht wird.

30.3.4 Lösungsansätze

Ich verkenne nicht, daß Verwaltungsdateien Grundlagen für statistische Auswertungen sein können; die geplante Volkszählung (siehe Nr. 30.1) ist ein Beispiel dafür. Nach meiner Einschätzung bieten sich folgende Lösungen an:

– **Bereichsspezifische Regelungen,** wenn in einem oder wenigen Bereichen die Datenverarbeitung der Verwaltung für Zwecke der Statistik genutzt und ggf. auch ausgeweitet werden soll. Allerdings muß sichergestellt werden, daß bei der Datenerhebung auf unterschiedliche Verwendungszwecke hingewiesen wird und daß fehlende statistische Angaben nicht zu einer Verzögerung oder Behinderung des Fachvorgangs führen dürfen – auch nicht bei statistischer Auskunftspflicht.

– **Eine Rahmenregelung,** wenn sich herausstellt, daß beispielsweise wegen rasch wechselnder Anforderungen der europäischen Statistik der Weg über Einzelgesetze zu aufwendig ist. Da über die Notwendigkeit, den Umfang und die Begleiterscheinungen der Statistik bereits im parlamentarischen Raum abgestimmt ist, könnte innerhalb eines vorgegebenen Rahmens ein einfacherer Verfahrensweg, etwa über eine Rechtsverordnung, vorgesehen werden. Dann werden zwar immer noch Vorschriften darüber benötigt, welche Stelle welche Daten für die Statistik zu übermitteln hat, aber der Beratungs- und Abstimmungsvorgang wird erleichtert.

Mit dieser Möglichkeit wird dem Ruf nach Verschlankung staatlicher Verwaltung genauso Rechnung getragen wie den Empfehlungen des Statistischen Beirates – ohne daß es einer allgemeinen und in ihren Folgen nicht abschätzbaren Ermächtigungsnorm für die Statistik bedarf.

31 Nicht-öffentlicher Bereich

31.1 Haushaltsbefragungen als Quelle für Direktmarketingdaten

Aufgrund der ursprünglichen Entwicklung der Informationstechnik wurden bislang Gefahren für die informationelle Selbstbestimmung der Bürger vor allem im Erheben, Verknüpfen und Auswerten von Bürgerdaten seitens des Staates gesehen. Vor diesem Hintergrund ist die Datenverarbeitung im öffentlichen Bereich nicht nur innerhalb des BDSG umfassender und strenger geregelt, sondern außerdem für viele Bereiche zusätzlich an bereichsspezifisches Datenschutzrecht gebunden worden. Die nunmehr verfügbaren technischen Möglichkeiten zur Informationsverarbeitung werden heute im nichtöffentlichen Bereich allerdings mindestens in gleichem Maße wie vom Staat ausgeschöpft. Die jetzige Situation ist dadurch gekennzeichnet, daß, je nachdem, ob staatliches Handeln oder Tätigkeiten privater Unternehmen zugrunde liegen, bei oftmals gleichen oder vergleichbaren Sachverhalten ein ganz unterschiedliches Datenschutzniveau besteht.

Ein anschauliches Beispiel hierfür sind **„Haushaltsbefragungen“,** in denen Bürger detailliert zu ihren privaten Lebensverhältnissen befragt werden.

Wird eine Haushaltsumfrage seitens des Staates durchgeführt – wie etwa beim Mikrozensus, einer Umfrage im Rahmen der amtlichen Statistik –, so sind die näheren Umstände, wie z. B. Art der Erhebung, Erhebungsmerkmale, Auskunftsverpflichtung der Bürger etc., im Mikrozensusgesetz detailliert geregelt (s. 16. TB Nr. 30.4.). Darüber hinaus sind die allgemeinen Regelungen des Bundesstatistikgesetzes zu beachten.

Auch wenn privaten Unternehmen die Möglichkeit fehlt, Bürger zur Beantwortung von Fragen zu verpflichten, sind privat durchgeführte Haushaltsbefragungen unter datenschutzrechtlichen Aspekten durchaus brisant. Denn der private Bereich ist hinsichtlich der näheren Gestaltung der Umfragen sowie der weiteren Verwendung der erhaltenen Daten kaum rechtlich geregelt. Daher können private Unternehmen ihre Fragen zu allen möglichen Lebensbereichen stellen (dies reicht von der Frage nach der Höhe des jährlichen Haushaltseinkommens bis zu der Frage, ob Schlankheitsmittel konsumiert werden) und die erhaltenen Informationen dann unbegrenzt verwenden, sofern nur der Befragte entsprechend eingewilligt hat.

Den Unternehmen stehen damit große Handlungsspielräume zur Verfügung, die sie selbstverständlich für ihre Geschäftszwecke nutzen. Um beispielsweise die Betroffenen zur Einwilligung zu bewegen, werden materielle Gegenleistungen angeboten, meist in Form von Verlosungen oder kleinen Geschenken. Zudem werden oft nett klingende oder gar verführerische Formulierungen gewählt, die es den Befragten schwer machen, sich auch der Nachteile und Risiken bewußt zu werden. Selbst wenn die Betroffenen über die vorgesehene Datennutzung aufgeklärt werden und insofern über ihre Daten „selbst bestimmt“ haben, bleibt bei dem Geschäft „personenbezogene Daten gegen heiße Preise“ ein schlechter Nachgeschmack, zumindest dann, wenn wegen der Art der abgefragten Daten und der Art ihrer Auswertung und Verbreitung doch zweifelhaft bleibt, ob die Betroffenen alle Risiken erkennen und richtig einschätzen können. Wenig bekannt ist u. a., daß die Freigabe für Marketingzwecke auch eine Verwendung im Ausland einschließen kann. So bietet die Direktmarketing-Industrie in den USA personenbezogene Informationen über deutsche

Verbraucher zum Kauf an, die für Werbezwecke weltweit genutzt werden können. Haben die Daten erst einmal diesen Weg genommen, sind sie dem Einfluß des Betroffenen – z. B. durch Widerspruch oder Löschungsanspruch – endgültig entzogen. Ebenso wenig ist bekannt, daß die Anbieter von Adressen letztlich keine Kontrolle darüber haben, ob die Daten tatsächlich ausschließlich für Werbezwecke oder etwa auch zur Kredit- oder Personalbeurteilung verwendet werden.

Umfangreiche privat veranlaßte Haushaltsbefragungen wurden im Berichtszeitraum nahezu zeitgleich von zwei großen deutschen Unternehmen durchgeführt. Die befragten Personen erhielten umfangreiche Fragebögen entweder per Postwurf oder persönliche Anschreiben und wurden gebeten, detaillierte Fragen zu Themen, wie z. B. Urlaubs- und Reisegewohnheiten, Freizeitaktivitäten, Gesundheit, Kauf- und Konsumverhalten, aber auch zur Schulbildung, beruflicher Tätigkeit sowie zur familiären und finanziellen Situation, zu beantworten (s. Abb. 12). Diese Konsumentenbefragungen dienten den Unternehmen – vielleicht nicht ausschließlich, aber doch wesentlich – zur Aktualisierung ihres vorhandenen Adressmaterialbestandes, den sie dann interessierten Unternehmen für Direktwerbungszwecke anbieten.

Diese „Verbraucher- bzw. Haushaltsumfragen“ stießen auf deutliche Kritik in den Medien und bei den zuständigen Aufsichtsbehörden, an die sich zahlreiche Bürger gewandt hatten. Deren Auffassung nach läßt die Gestaltung der Fragebögen weder Sinn und Zweck der Erhebungen noch die weitere Verwendung der Angaben deutlich genug erkennen. Sie sehen neben der Beeinträchtigung schutzwürdiger Belange der Betroffenen auch die erforderliche Transparenz und Aufklärung, die für eine informierte Einwilligung erforderlich sind, als nicht gegeben. Im Gegensatz zu statistischen Auswertungen oder produktbezogenen Marktforschungen, bei denen es ausreicht, daß die Angaben im weiteren Verfahren anonym zur Verfügung stehen, erlauben die beschriebenen Umfragen durch ihre doppelte Zwecksetzung – Marktforschung und Direktwerbung – den Personenbezug zu erhalten und damit ein Persönlichkeitsprofil des Betroffenen zu erstellen und ihn dadurch zu einem „gläsernen Kunden“ zu machen.

Die Aufsichtsbehörden haben daraufhin Mindestanforderungen für derartige Datenerhebungen beschlossen. Danach muß klar erkennbar sein, daß die Angaben nicht nur anonym, sondern auch personenbezogen ausgewertet werden sollen. Ebenso deutlich muß sein, welchen Zwecken ihre Verwendung dient, etwa persönlich adressierter Werbung. Um sicherzustellen, daß der Betroffene seine Entscheidung zur Auskunftserteilung in voller Kenntnis der Sachlage trifft, ist eine schriftliche Einwilligung auf dem Erhebungsbogen selbst notwendig. Diese müssen alle volljährigen bzw. einsichtsfähigen Personen erklären, auf die sich die erbetenen Angaben beziehen.

Es bleibt abzuwarten, ob es gelingt, diese Anforderungen tatsächlich umzusetzen. Ich meine, daß bei der Bewertung derartiger Umfragen unter Datenschutzgesichtspunkten der Transparenz für den Betroffenen eine durchschlagende Bedeutung zukommt. Der Betroffene muß wissen, was er tut, wenn er Informationen über sein Privatleben preisgibt. Vor allem muß klar erkennbar sein, was mit seinen Daten geschehen wird, wohin sie fließen und für welche Zwecke sie verwendet werden können. Nur dann kann er abschätzen, welche Folgen dies für ihn haben kann.

Wenn die Unternehmen diese Transparenz gewährleisten, habe ich keine Bedenken. Falls sie jedoch nicht bereit sein sollten, hier offen und fair zu agieren, sollte im Zusammenhang mit der Novellierung des BDSG (s. o. Nr. 2.1.2) eine verschärfte gesetzliche Regelung zum Schutze der Bürger die Folge sein.

31.2 Neue Entwicklungen bei der Kreditinformation

Der Markt für Kredite und auf Kredit gewährte Produkte und Dienstleistungen wächst stetig. Zu den traditionellen Bankkrediten und Leasinggeschäften treten kreditähnliche Vorleistungen und Ausfallrisiken, besonders in Zukunftsmärkten wie Mobilfunk, Online-Diensten und Teleshopping. Damit ist auch ein erweiterter Bedarf für Bonitätsprüfungssysteme entstanden.

Bislang ist die Schufa das einzige größere Kreditinformationssystem für Endverbraucher in Deutschland. Kurz vor dem Abschluß stehen nunmehr die Planungen für ein neues, umfassend angelegtes Informationssystem über die Kreditwürdigkeit und -fähigkeit von Privatpersonen. Während bei der Schufa eine Vertragspartnerschaft auf Unternehmen der Geld- und Warenkreditvergabe beschränkt ist – eine Ausnahme besteht lediglich für Mobilfunkanbieter, deren Kreditrisiko als vergleichbar hoch eingeschätzt wird –, soll bei dem neuen System der Kreis der Vertragspartner erheblich weiter gezogen werden. Vom Einzelhandel über den Versandhandel, Versicherungen und Telekommunikationsunternehmen bis hin zu Bausparkassen und Banken stellt man sich den Kreis der Vertragspartner vor.

Die dem System angeschlossenen Vertragspartner sollen verpflichtet werden, ihrerseits Informationen über das Zahlungsverhalten ihrer Kunden an das Informationssystem zu liefern. Auch ist geplant, die branchenübergreifenden Informationen der Vertragspartner mit öffentlichen Informationen (eidesstattlichen Versicherungen, Haftbefehlen, Konkursen, Vergleichen usw.), Inkassodaten des Unternehmens sowie weiterer Datenbanken zu verknüpfen. Ferner ist vorgesehen, auch Informationen aus den Mikrotypdaten (soziodemographische Beschreibung des Wohnumfeldes des Betroffenen, zusammengefaßt in Einheiten von mindestens fünf Haushalten) zu verwenden und die Daten über das Zahlungsverhalten mit integrierten Risiko-Management-Lösungen zu verbinden. Darüber hinaus werden auch Verfahren wie Kredit-Scoring, Verhaltens-Scoring und Customer-Scoring angeboten.

Es handelt sich hier ohne Zweifel um eine neue Dimension der Datenkonzentration. M.E. ist unter Datenschutzgesichtspunkten daher vor allem Transparenz gegenüber dem Betroffenen und Freiwilligkeit hinsichtlich der Einwilligung zu einer Datenübermittlung zu fordern.

Abbildung 12 (zu Nr. 31.1)

Auszug aus einem Fragebogen

7. EINKAUFEN

1. In welchen der folgenden Geschäfte kaufen Sie in der Regel Lebensmittel bzw. Güter des täglichen Bedarfs ein?

Aldi	01	HL-Markt	10	Kromm/Krone	19	Penny	28
Allkauf	02	Horten	11	Ledi	20	Plus	29
Dixi	03	Inter-/Eurospar	12	Lidl	21	Real	30
Edeka	04	Kaiser's	13	Magnet	22	Rewe	31
Extra	05	Karstadt	14	Marktkauf	23	Spar	32
Globus	06	Kaufhalle	15	MiniMal	24	Tengelmann	33
Grosso	07	Kaufhof	16	MultiCenter	25	Toom	34
Handelshof	08	Kaufland	17	Netto	26	Wertkauf	35
Hertie	09	Kontra	18	Norma	27	andere	36

2. In welchen der folgenden Drogerien/Drogeriemärkte kaufen Sie meistens ein?

Fachhandels-Drogerie	01	Idea	05	Müller	09
Budnikowski	02	Ihr Platz	06	Schlecker	10
dm	03	kd	07	Sconti	11
Drospa/Fuchs	04	Kloppenburg	08	andere	12

3. Welche Eigenschaften sind für Sie beim Einkaufen wichtig?

	sehr wichtig	wichtig	weder noch	unwichtig
Preis	01	02	03	04
Qualität	05	06	07	08
Sortiment	09	10	11	12
bekannte Marken	13	14	15	16
Beratung	17	18	19	20

4. Wie oft kaufen Sie Tiefkühlkost ein?

mind. 1 x pro Woche 1 | mehrmals i. Monat 2 | 1 x im Monat 3
seltener 4 | nie 5

5. In welchen der folgenden Baumärkte kaufen Sie normalerweise ein?

Bahr	01	Hagebaumarkt	09	Profi	17
Baufuchs	02	Hauser	10	Stinnes	18
Bauhaus	03	Hellweg	11	Toom	19
Bauklotz/Werkmarkt	04	Hornbach	12	Topbau	20
Castorama	05	Krone	13	Wierichs	21
Extra Bau+Hobby	06	Mobau	14	andere	22
Globus	07	Obi	15	in keinem	23
Götzen	08	Praktiker	16		

6. Welche Damen-Konfektionsgrößen werden in Ihrem Haushalt hauptsächlich gekauft?

34/36	1	46/48	4	Kurzgrößen	7
38/40	2	50/52	5	Langgrößen	8
42/44	3	54/56	6	andere	9

17. Wie viele Maschin

keine 1 1-

18. Welchen Weichspü

Lenor 1
Vernel 2

19. Welchen Haartyp g

trockenes 1
normales 4

20. Welche Haarpflege

Shampoo 1
Schaumfestiger 4
Gel 7

21. Welche der folgend

Haarspray 1

22. Welche Marke für am häufigsten ve

AoK 1
Florena 4
Ponds 7

23. Welche der folgen Sie in den letzten

Margaret Astor 01
Avon 02
Ellen Betrix 03
Chanel 04
Chicogo 05

24. Wie häufig werden

min. pro Wo

Albi 01
Aldi 02
Granini 03
Hohes C 04
Punica 05

25. Wie viele Flasche

Albi 01
Aldi 02

Der Betroffene, der um seine Einwilligung gebeten wird, muß darüber aufgeklärt werden, welche Daten zu seiner Person gespeichert werden sollen und welchem potentiellen Empfängerkreis diese Daten zur Verfügung stehen. Die Einwilligung selber muß auf freiwilliger Basis erfolgen. Ein Konditionenkartell aller Anbieter derart, daß bestimmte Arten von Produkten oder Leistungen nur unter Erteilung der Einwilligung angeboten werden – was für den Kunden einen faktischen Zwang bedeutet – darf es nicht geben. Darüber hinaus ist bei der Konzeption des Systems darauf zu achten, daß die anfragenden Vertragspartner nur im Rahmen ihres jeweiligen berechtigten Interesses Informationen erhalten. Eine Vermischung zwischen Bonitätsprüfungsinteresse und Interesse an Direktmarketing muß ausgeschlossen sein.

Eine abschließende Bewertung der obersten Aufsichtsbehörden lag bei Redaktionsschluß noch nicht vor. Die Diskussion der Aufsichtsbehörden untereinander sowie mit den beteiligten Unternehmen dauert an.

31.3 Ringen um ein Mehr oder Weniger an Datenschutz: Allfinanzklauseln und Scoring-Verfahren

Der Dialog zwischen Aufsichtsbehörden und Vertretern der Wirtschaft gestaltet sich immer dann besonders schwierig, wenn es darum geht, sich auf ein bestimmtes Datenschutzniveau zu einigen. Die eher traditionell denkenden Branchen der Wirtschaft zeigen hier bedauerlicherweise eine mehr restriktive Haltung. Statt eine datenschutzfreundliche Anwendung von Datenverarbeitungsverfahren zu forcieren und dies als Marketingargument zu nutzen, wird bei nahezu jedem neuen Vorhaben mit den Aufsichtsbehörden zäh um ein Mehr oder Weniger an Datenschutz gerungen.

Ein Beispiel hierfür ist die Ausgestaltung der **Allfinanzklauseln** in der Kreditwirtschaft. Diese bereitete in den Verhandlungen zwischen Aufsichtsbehörden und Kreditwirtschaft große Schwierigkeiten. Man einigte sich schließlich auf die Schriftform und die drucktechnische Hervorhebung der Einwilligungserklärung, sofern diese mit anderen Erklärungen, z. B. mit der Einverständniserklärung zu den AGB, zusammengefaßt ist (s. 16. TB Nr. 31.2.4). Dies ist nach derzeit geltendem Recht ein nicht zu beanstandendes Ergebnis. Im Interesse der Bankkunden wären hingegen weitergehende Vorkehrungen wünschenswert gewesen. Die Kreditwirtschaft ließ sich jedoch bisher nicht dazu bewegen, durch geeignete Maßnahmen, wie z. B. durch eine gesonderte Unterschrift oder durch Ankreuzen, sicherzustellen, daß der Einwilligende die Erklärung auch tatsächlich zur Kenntnis genommen und eine bewußte Auswahlentscheidung getroffen hat. Es wird sich zeigen, ob dieses Resultat den Vorgaben der EG-Richtlinie (s. o. Nr. 2.1.1) standhalten wird, die für die Einwilligung fordert, daß diese für den konkreten Fall und in Kenntnis der Sachlage erfolgt („informed consent“, Artikel 2 Buchstabe. h).

Ähnlich unbefriedigend verhält es sich beim **Scoring-Verfahren der Schufa.** Bei diesem Verfahren wird aus einem Datenbestand mittels mathematisch-statistischer Verfahren ein Scorewert erstellt, der die Wahrscheinlichkeit für den Eintritt eines bestimmten Ereignisses wiedergibt .Die Aufsichtsbehörden haben – was ich schon problematisiert habe (s. 16. TB Nr. 31.2.3) – eine datenschutzrechtlich relevante Beeinträchtigung schutzwürdiger Belange der Betroffenen durch das Scoring-Verfahren verneint und lediglich einige Empfehlungen an die Schufa ausgesprochen. So empfahlen sie, einen Hinweis auf das Scoring-Verfahren in das Merkblatt zur Schufa-Klausel aufzunehmen sowie sicherzustellen, daß ihre Vertragspartner den Scorewert allein zugunsten der Kreditnehmer nutzen und im Falle eines Auskunftsbegehrens das Scoring-Verfahren allgemein erläutern.

Ich teile nach wie vor nicht die von der Schufa in ihrem Merkblatt für den Betroffenen gemachte Aussage, daß die in einem Scorewert zusammengefaßte Prognose keine Bewertung der Bonität eines konkreten Kunden darstelle.

Die Schufa fügt durch die Bildung eines Scorewertes den Daten des Betroffenen einen zusätzlichen Wert hinzu. Dieser beruht zwar auf im Schufa-Bestand enthaltenen Erfahrungen mit Kredtiverläufen anderer Schuldner (mit ähnlichen Merkmalen). Er wird aber von der Schufa den Daten des konkret beauskunfteten Kunden beigefügt, weil dies dem anfragenden Vertragspartner im Massengeschäft die Abwicklung erleichtert. Der Scorewert ermöglicht einen Vergleich mit anderen Schuldnern und Kreditsuchenden und ordnet dem einzelnen eine Position innerhalb einer Bezugsgruppe zu; damit hat er aus meiner Sicht den Charakter einer Bewertung.

Unabhängig von der Einstufung als Bewertung, die nach der Umsetzung der EG-Datenschutzrichtlinie Artikel 15 und Artikel 12 a) 3. Anstrich von großer Bedeutung sein wird, stellen die Scorewerte personenbezogene Daten dar, auf deren Bekanntgabe der Betroffene einen Anspruch hat (§ 34 Abs. 1 und 2 BDSG). Die Scorewerte werden den Kreditgebern als Grundlage für die Entscheidung über einzelne Kreditanträge einzelner Betroffener zur Verfügung gestellt. Damit hilft die Schufa nach eigenem Bekunden, *„Kreditentscheidungen objektiv und rationell zu treffen“* (www.schufa.de/Verbraucher/index.htm). Warum sie gleichwohl geltend macht, der Scorewert sei nicht auf eine einzelne Person zugeschnitten, sondern eine gruppenbezogene Prognose und daher kein personenbezogenes Datum, ist für mich nicht nachvollziehbar.

Ich halte Transparenz für die Betroffenen für unverzichtbar und appelliere an die Beteiligten, diese auch unabhängig von einer rechtlichen Verpflichtung herzustellen, zumal dies letztlich auch im Interesse der Kreditwirtschaft selbst liegt. Über Einzelheiten – wie z. B. die Einbeziehung der Kreditinstitute und die Aufklärung der Betroffenen über das Verfahren und ihre Rechte – sollte möglichst bald Einvernehmen zwischen den Aufsichtsbehörden und der Schufa sowie der Kreditwirtschaft hergestellt werden.

Ein „Mehr“ an Datenschutz ist auch hier nach wie vor dringend wünschenswert.

31.4 Bekannte Probleme in neuem Kontext: Wirtschaftsinformationen im Internet und Outsourcing durch Banken

Vor dem Hintergrund einer sich herausbildenden Informationsgesellschaft muß das vorhandene rechtliche Instrumentarium immer wieder neu angewandt werden, um technische Entwicklungen und neue Verfahren datenschutzrechtlich einbinden und begleiten zu können. Subsumtion und Auslegung des Datenschutzrechts sind nicht eng begrenzt, sondern eröffnen Spielräume, die es erlauben, auch mit neuen Fallgestaltungen und technischen Entwicklungen flexibel und datenschutzfreundlich umzugehen.

Neue Wege eröffnen sich etwa bei allgemein zugänglichen **Datenbanken.** So stellt ein privates Unternehmen, das die im Bundesanzeiger veröffentlichten Handelsregisterauszüge auswertet, diese Daten in eine Datenbank ein, um sie via Internet Dritten ohne Übernahme rechtlicher Gewähr zugänglich zu machen. Dieses Verfahren birgt wegen der technischen Möglichkeiten moderner Datenverarbeitung, insbesondere der vielfältigen Recherche- und Verknüpfungsmöglichkeiten, ganz neue Nutzungsmöglichkeiten, etwa zur Erstellung von Informationsprofilen oder zum Abruf mit Merkmalen (z. B. Adressen), bei denen zweifelhaft ist, ob sie vom Zweck des Handelsregisters gedeckt sind. Die Aufsichtsbehörden lehnen sich eng an das geltende Recht an und halten das Verfahren für rechtlich unzulässig, da auf den nach dem BDSG erforderlichen Nachweis eines berechtigten Interesses verzichtet wird. Allerdings haben auch sie Zweifel, ob damit der Publizität des Handelsregisters hinreichend Rechnung getragen wird. Da die Daten aus allgemein zugänglichen Quellen stammen, können schutzwürdige Belange erst durch das Hinzutreten weiterer Umstände, etwa durch die Verknüpfung mit anderen, nicht aus dem Handelsregister stammenden Informationen, beeinträchtigt werden.

Auch dieses Beispiel zeigt, daß das Thema Publizität im Zeitalter des Internet aus Datenschutzsicht generell neu zu überdenken ist. Die Konsequenz sehe ich aber nicht in einem Abbau von Öffentlichkeit oder einer generellen Einschränkung der datenschutzrechtlichen Erlaubnis zur Nutzung publizierter personenbezogener Daten. Vielmehr muß von Fall zu Fall genau überprüft werden, welcher Sinn und Zweck der Publizität zukommt. Geht es nur darum, durch Öffentlichkeit des Verfahrens dessen Legitimität oder Kontrollierbarkeit zu sichern, wie etwa bei der Auslegung von Wählerverzeichnissen oder dem (mittlerweile abgeschafften) Aushang von Ehe-Aufgeboten, so besteht keinerlei innere Rechtfertigung, die Verwendung der betreffenden Daten auch zu ganz anderen Zwecken in einem ganz anderen zeitlichen Zusammenhang freizugeben. Das Fehlen entsprechender differenzierter Regelungen wird durch die veränderte Informationstechnik immer mehr offenkundig und die gesetzgeberische Reaktion daher notwendig. Dagegen kann es durchaus auch Fälle geben, bei denen Publizität ohne Wenn und Aber gewollt oder geboten ist, so daß auch neue Auswertungsmöglichkeiten durchaus der gesetzlichen Intention entsprechen. Die Klärung, wie insoweit das Handelsregister einzuordnen ist, steht noch am Anfang. Ich neige aber dazu, die Einstellung des Registers selbst in das Internet grundsätzlich als mit der Zielsetzung des Handelsregisters vereinbar anzusehen.

Auch hinsichtlich des Themas **„Outsourcing“** ist der Datenschutz neu auszuloten. Wegen der zunehmenden Arbeitsteilung im Wirtschaftsleben gibt es hier vielfältige Vorhaben. Im Bankenbereich ist man beispielsweise bestrebt, Wertpapiergeschäfte und die Wertpapierverwahrung zentral über andere Banken abzuwickeln, oder es werden Markt- und Meinungsforschungsinstitute mit Kundenbefragungen beauftragt, um das eigene Dienstleistungsangebot zu überprüfen und ggf. zu verbessern. Bei der jeweils erforderlichen Weitergabe personenbezogener Daten ist rechtlich danach zu differenzieren, ob es um **„Funktionsübertragungen“** oder um **„Datenverarbeitung im Auftrag“** geht. Im ersten Fall handelt es sich rechtlich um eine Übermittlung, womit die Einholung einer Einwilligung bei allen Betroffenen nötig werden kann. Bei den Aufsichtsbehörden überwog bisher die Auffassung, daß die Auftragsvorschriften dann nicht anzuwenden sind, wenn der Auftrag über eine praktisch-technische Hilfeleistung („bloße Datenverarbeitung“) hinausgeht – etwa eine komplexe Sachbearbeitung. Dagegen steht die – auch von mir unterstützte – Auffassung, daß Datenschutzbelange besser gewahrt sind, wenn den Betroffenen ihr (Vertrags-)Partner als alleinige datenschutzverantwortliche Stelle erhalten bleibt. Notwendig, aber auch ausreichend ist es, dem beauftragten Dritten in puncto Datenschutz genaue verfahrensmäßige und technische Vorkehrungen zur Behandlung der personenbezogenen Daten verbindlich vorzugeben.

Ein moderner Datenschutz muß der steigenden Bedeutung des Outsourcing im öffentlichen wie im nicht-öffentlichen Bereich für eine wirtschaftliche und effiziente Aufgabenerfüllung Rechnung tragen. Der Datenschutz soll der Optimierung von Arbeitsabläufen nicht im Wege stehen. Andererseits darf der Datenschutz auch nicht durch Oursourcing geschwächt werden. Um beides zu erreichen, müssen vor allem die Vorschriften über Berufs- und besondere Amtsgeheimnisse so umgestaltet werden, daß der durch sie garantierte gesteigerte Schutz auch im Falle des Outsourcing erhalten bleibt.

31.5 Der „Düsseldorfer Kreis“ wurde 20 Jahre alt

Das Jubiläum des „Düsseldorfer Kreises“, der im Herbst 1997 auf sein 20jähriges Bestehen zurückblicken konnte, bot Anlaß, über Vergangenes und Kommendes beim Datenschutz im nicht-öffentlichen Bereich zu reflektieren. 20 Jahre zuvor, im Herbst 1977, waren die Vertreter der obersten Aufsichtsbehörden der Länder für den Datenschutz im nicht-öffentlichen Bereich zum ersten Mal in Düsseldorf zusammengekommen. Sinn und Zweck war ein Erfahrungsaustausch, um eine möglichst einheitliche Anwendung des kurz zuvor verabschiedeten ersten Bundesdatenschutzgesetzes sicherzustellen. So entstand der „Düsseldorfer Kreis“ – ein ständiges Koordinationsgremium der obersten Aufsichtsbehörden der Länder für den Datenschutz. Die Themen haben sich im Laufe der Jahre stark verändert. Ging es anfangs um die Interpretation der

Rechtsbegriffe und Bestimmungen des BDSG, so stellten sich im Zuge technischer Innovation und europäischer Rechtsangleichung neue Themen, beispielsweise aus den Bereichen Teledienste, Chipkartenanwendungen oder Datenbanken im Internet. Ein Schwerpunktthema sind die Beratungen zur EG-Datenschutzrichtlinie vom 24. Oktober 1995. Die Aufsichtsbehörden sehen großen Reformbedarf bei der Novellierung des BDSG, der über die sich aus der Richtlinie ergebenden Rechtsänderungen weit hinausgeht (s. o. Nr. 2.1.2).

32 Internationale Zusammenarbeit und Datenschutz im Ausland

32.1 Datenschutz im Europarat

Dem „Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten" – der Europaratskonvention 108 aus dem Jahre 1981 – traten im Berichtszeitraum zwei weitere Mitgliedstaaten des Europarats bei. Im Oktober 1997 ratifizierten die Schweiz und Ungarn die Konvention, die in beiden Ländern am 1. Februar 1998 in Kraft getreten ist. Damit erhöhte sich die Zahl der Staaten, in denen das Übereinkommen gilt, auf 20, womit genau die Hälfte der mittlerweile 40 Mitgliedstaaten des Europarats der Konvention beigetreten ist. Nach einer entsprechenden Entscheidung des Rates der Europäischen Union vom Juli 1997 hat auch die Kommission Verhandlungen über einen Beitritt der Europäischen Gemeinschaft zur Konvention 108 aufgenommen.

Das Ministerkomitee nahm nach jahrelangen Vorarbeiten (vgl. 16. TB Nr. 32.1) in der Projektgruppe Datenschutz (CJ-PD) und ihren entsprechenden Untergruppen sowie im Lenkungsausschuß für rechtliche Zusammenarbeit (CDCJ) zwei weitere Empfehlungen an. Die Empfehlung Nr. R (97) 5 vom 13. Februar 1997 zum Schutz medizinischer Daten tritt an die Stelle der aus dem Jahre 1981 stammenden Empfehlung Nr. R (81) 1 betreffend Vorschriften für automatisierte medizinische Datenbanken. Die Empfehlung Nr. R (97) 18 vom 30. September 1997 zum Schutz personenbezogener Daten, die für statistische Zwecke erhoben und verarbeitet werden, ersetzt teilweise die Empfehlung Nr. R (83) 10 betreffend den Schutz personenbezogener Daten, die für wissenschaftliche Forschung und Statistik verwendet werden. Weiterhin im Entwurfsstadium (vgl. 16. TB Nr. 32.1) – wenn auch inzwischen auf der Ebene der Projektgruppe Datenschutz (CJ-PD) – befindet sich eine Empfehlung zum Schutz personenbezogener Daten bei der Erhebung und Verarbeitung für Versicherungszwecke.

Der durch das Europaratsübereinkommen ins Leben gerufene Beratende Ausschuß (T–PD) zur Anwendung der Konvention 108 begann mit Vorüberlegungen zur Überarbeitung des Übereinkommens im Lichte des technischen Fortschritts und der Entwicklungen der letzten Jahre. Beraten wurde zunächst die Verarbeitung von Tonträgern und Bildern sowie die Verarbeitung von Daten, die Verstorbene betreffen.

32.2 Ein Blick in europäische Länder außerhalb der Union

32.2.1 Der Europäische Wirtschaftsraum

Nach der Aufnahme in das Abkommen über den Europäischen Wirtschaftsraum (EWR) wird die europäische Datenschutzrichtlinie in allen seinen Mitgliedstaaten wirksam werden. Die Arbeiten für die Umsetzung sind bei den Nicht-EU-Mitgliedern des Abkommens **Norwegen** und **Island** bereits in die Wege geleitet worden. In Norwegen, dessen Datenschutzgesetz aus dem Jahre 1978 stammt, wie in Island, das seit 1981 ein Datenschutzgesetz besitzt, haben Parlamentsausschüsse mit der Prüfung der Notwendigkeit von Anpassungen der bestehenden Gesetze an die Regelungen der EG-Richtlinie begonnen. Beide EWR-Mitgliedstaaten sind bereits der Datenschutzkonvention (Übereinkommen Nr. 108) des Europarats (s. o. Nr. 32.1) beigetreten. Die Vertreter der Datenschutzbehörden beider Länder werden zu den Sitzungen der Brüsseler Datenschutzgruppe nach Artikel 29 der EG-Richtlinie (s. o. Nr. 2.2) als Beobachter eingeladen.

32.2.2 Die Staaten Mittel- und Osteuropas

Bereits in zurückliegenden Tätigkeitsberichten (15. TB Nr. 33.3, 16. TB Nr. 32.3.2) konnte ich über gesetzgeberische Bestrebungen auf datenschutzrechtlichem Gebiet in zahlreichen mittel- und osteuropäischen Ländern (MOE-Staaten) berichten.

Mit seinem 1993 in Kraft getretenen Datenschutzgesetz bildete **Ungarn** den Vorreiter. Zwar war schon am 1. Juni 1992 in der damaligen Tschechoslowakischen Republik ein Gesetz über den Schutz personenbezogener Daten in Informationssystemen in Kraft getreten, doch sah dieses Gesetz keine eigenständige Regelung für eine unabhängige Kontrollstelle vor.

Nach seiner vorübergehenden Weitergeltung über die Auflösung des tschechoslowakischen Staates hinaus wurde das Gesetz im Februar 1998 in der **Slowakei** durch ein neues Datenschutzgesetz abgelöst, das sich eng an die Regelungen der EG-Richtlinie (s. o. Nr. 2.1.1) anlehnt. Es gilt für automatisierte und manuelle Dateien und sieht die Einrichtung einer Kontrollstelle innerhalb der Informationsabteilung des Statistischen Amtes der Slowakei vor.

Dagegen gilt in der **Tschechischen Republik** nach wie vor das aus dem Jahre 1992 stammende Gesetz. In seinem § 24 geht es weiterhin davon aus, daß erst durch ein besonderes Gesetz Organe geschaffen werden, die für die Registrierung und Überwachung des Betriebes der Informationssysteme zuständig sind. Der tschechische Gesetzgeber hat jedoch bis heute von dieser Ermächtigungsvorschrift keinen Gebrauch gemacht. Über die damit zusammenhängenden Probleme beim Aufbau eines glaubwürdigen Datenschutzsystems konnte ich mich anläßlich eines Informationsbesuchs auf Einladung des tschechischen Innenministeriums im Sommer 1998 vor Ort unterrichten. In Gesprächen mit dem stellvertretenden Innenminister, der die Begegnung als „historisch"

wertete, sowie mit Behördenleitern von Polizei-, Grenzpolizei- und Zolldienststellen konnte ich mir ein Bild über die Bemühungen um den Datenschutz in einer derartigen Übergangsphase machen. Großes Interesse zeigten die tschechischen Gastgeber darüber hinaus an einem Gedankenaustausch über die europäischen Vorgaben nach der EG-Richtlinie und im Hinblick auf EUROPOL und Schengen sowie über meine eigenen datenschutzrechtlichen Erfahrungen aus deutscher Sicht.

In **Polen** wurde im August 1997 ein stark an der EG-Richtlinie orientiertes Datenschutzgesetz verabschiedet, welches im April 1998 in Kraft getreten ist. Die Datenschutzgrundsätze sind in der im Oktober 1997 in Kraft getretenen neuen polnischen Verfassung in ihren Artikel 49 bis 51 verankert. Mit der im vergangenen Jahr vom Sejm ernannten ersten Datenschutzbeauftragten, Frau Dr. Kulesza, fand bereits ein reger Informations- und Gedankenaustausch statt. Ein Student der Staatlichen Verwaltungsakademie in Warschau absolvierte ein Praktikum in meiner Dienststelle. Dabei entstand auch eine deutsche Übersetzung des polnischen Datenschutzgesetzes (abgedruckt in der Zeitschrift Datenschutz und Datensicherheit 1998, S. 463 ff.).

Gesetzgeberische Vorhaben auf Kabinetts- oder Parlamentsebene gibt es derzeit in **Bulgarien, Lettland, Moldawien** und **Rumänien.**

32.3 Entwicklungen im nicht-europäischen Ausland

Eine vom spanischen Datenschutzbeauftragten im Frühjahr 1997 in Madrid veranstaltete **europäisch-lateinamerikanische Datenschutzkonferenz** bildete erstmals ein gemeinsames Forum für einen Gedankenaustausch zwischen europäischen Datenschutzbeauftragten und Vertretern von Innen- und Justizministerien der meisten Staaten Mittel- und Südamerikas. Wie schon auf der Konferenz angekündigt, beschloß die **Ibero-amerikanische Konferenz der Justizminister** im Juni 1998, den Entwurf eines Modellgesetzes über den Datenschutz zu prüfen. In **Argentinien** hatte 1997 eine parlamentarische Kommission die Annahme eines Gesetzentwurfs zum Datenschutz (Habeas Data Bill) empfohlen, der von beiden Häusern des Parlaments angenommen wurde. Der Präsident legte jedoch sein Veto ein mit der Begründung, daß die in dem Entwurf vorgesehenen Regelungen der Wirtschaft und insbesondere den Großunternehmen schaden würden. Seitdem sind im Kongreß mehrere neue Entwürfe eingebracht worden, ohne daß bislang Fortschritte erzielt worden wären. In **Brasilien** wurde der Entwurf eines Datenschutzgesetzes im Parlament eingebracht, mit dessen Beratungen jedoch noch nicht begonnen wurde.

Auf dem nordamerikanischen Kontinent (zu den **USA** und insbesondere der transatlantischen Debatte über den Drittstaaten-Transfer s. o. Nr. 2.2.2) hat die **kanadische** Bundesregierung im Rahmen ihrer Ankündigung, ein Gesetzespaket für den Datenschutz im privaten Sektor vorzulegen, im Oktober 1998 einen entsprechenden Gesetzentwurf im Parlament eingebracht. Die Provinzen mit Ausnahme **Quebecs,** dessen Datenschutzgesetz aus dem Jahre 1993 als bisher einziges in Kanada auch für den nicht-öffentlichen Bereich gilt (vgl. 16. TB Nr. 32.3.3), haben sich jedoch bisher noch nicht bereit gefunden, im Rahmen ihrer Zuständigkeitsbereiche für den Privatsektor gleichzuziehen.

In **Israel** verabschiedete die Knesset weitreichende Änderungen zu dem seit 1981 geltenden Datenschutzgesetz. Durch die Novelle, über deren Entwurf ich im 16. TB (Nr. 32.3.4) berichtet habe, wurden u. a. Regelungen zum Direktmarketing eingefügt. Danach kann der Betroffene Löschung der ihn betreffenden personenbezogenen Daten verlangen, die in einer zu Zwecken des Direktmarketings angelegten Datenbank gespeichert sind. Direktmarketing-Veranstaltungen müssen für den Betroffenen als solche erkennbar gemacht und dabei die Herkunft der Daten angegeben werden.

In **Australien** beabsichtigt die Bundesregierung eine Erweiterung des seit 1988 bestehenden Privacy Act, wobei insbesondere die Bestimmungen über den nicht-öffentlichen Bereich novelliert werden sollen. Zu diesem Zweck hat die Regierung ein detailliertes Diskussionspapier mit Datenschutzprinzipien vorgestellt, die an gesetzliche Regelungen in **Neuseeland** und **Hongkong** (vgl. 15. TB Nr. 33.3 und 16. TB Nr. 32.3.3) angelehnt sind und Überlegungen der europäischen Datenschutzrichtlinie (s. o. Nr. 2.1.1), insbesondere im Hinblick auf die Erhebung und Speicherung von Daten, die Betroffenenrechte und die Datenübermittlung in Drittländer, aufgreifen. Auf einzelstaatlicher Ebene wird in **Victoria** ein Gesetz beraten, das subsidiär immer dann eingreifen soll, wenn die Selbstkontrolle in der Praxis versagt. Hiermit würde erstmals ein Versuch unternommen, verschiedene Datenschutzkonzepte miteinander zu verbinden.

Das **japanische** Datenschutzgesetz aus dem Jahre 1990 gilt nur für den öffentlichen Bereich. Im März 1997 verabschiedete das Ministerium für Handel und Industrie (MITI) sog. Leitlinien für die Datenverarbeitung im privaten Bereich. Die Leitlinien orientieren sich an dem Übereinkommen des Europarats zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten – der Konvention 108 – aus dem Jahre 1981 (s. o. Nr. 32.1) und an den Leitlinien der Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD) für den Schutz des Persönlichkeitsbereichs und den grenzüberschreitenden Verkehr personenbezogener Daten aus dem Jahre 1980, stellen dabei aber Selbstregulierungsmaßnahmen der Wirtschaft in den Vordergrund. Hierüber sowie über Fragen des Drittstaatentransfers nach Ländern außerhalb der EU (s. o. Nr. 2.2.2) fand ein Gedankenaustausch mit Mitgliedern des japanischen Repräsentantenhauses in meiner Dienststelle statt.

In **Malaysia** hat das Parlament einen Ausschuß für die Erarbeitung eines Entwurfs für ein Datenschutzgesetz ernannt. Das Gesetz soll für den öffentlichen und für den privaten Bereich gelten und die Verarbeitung in automatisierten wie in manuellen Dateien regeln. Die Einrichtung einer unabhängigen Datenschutzkontrollinstanz soll ein weiteres wesentliches Ziel des Gesetzes sein.

32.4 Die Internationale Datenschutzkonferenz

Die 19. Internationale Konferenz der Datenschutzbeauftragten vom 17. bis 19. September 1997 in Brüssel war überwiegend auf europäische Datenschutzfragen ausgerichtet. Themenschwerpunkte bildeten der grenzüberschreitende Datenverkehr nach Ländern außerhalb der EU und das dabei nach den Artikel 25 und 26 der EG-Richtlinie einzuhaltende angemessene Schutzniveau im Drittstaat (s. o. Nr. 2.2.2), Datenerhebungen im Polizeibereich (Schengen, EUROPOL und INTERPOL) und das Spannungsfeld Datenschutz und Pressefreiheit, insbesondere im Hinblick auf die Vorgaben von Artikel 9 der EG-Richtlinie. Ein weiteres Konferenzthema war dem Internet gewidmet. In einem Redebeitrag habe ich über jüngste Entwicklungen bei Telekommunikation und Telediensten in Deutschland berichtet und dabei insbesondere das TKG und das IuKDG vorgestellt.

Themen des nicht-öffentlichen Bereichs bildeten einen Schwerpunkt der 20. Internationalen Datenschutzkonferenz vom 16. bis 18. September 1998 in Santiago de Compostela (Spanien). Dabei wurden Fragen öffentlich zugänglicher Daten (etwa aus Wählerverzeichnissen oder Telefonbüchern) und ihrer Verwertung für Zwecke der Werbung und des Direktmarketings diskutiert sowie der Umgang mit personenbezogenen Daten zur Bestimmung der Kreditwürdigkeit von Bankkunden. Ferner wurden Datenschutzprobleme im elektronischen Geschäftsverkehr und bei der Nutzung von E-Mail sowie im Zusammenhang mit der Erhebung von Mautgebühren (Road Pricing) erörtert.

Erneut wurde die europäische Datenschutzrichtlinie im Hinblick auf den Drittstaatentransfer (s. o. Nr. 2.2.2) diskutiert. Ein weiteres Thema bildeten die sog. sensitiven Daten nach Artikel 8 der Richtlinie (vgl. 15. TB Nr. 33.1.4.5). Hierzu habe ich in einem Redebeitrag über Sozial- und Gesundheitsdaten auf die europäischen Vorgaben hingewiesen und ihre Auswirkungen auf die Novellierung des BDSG deutlich gemacht.

Schließlich verabschiedeten die Datenschutzbeauftragten der Mitgliedstaaten der Europäischen Union gemeinsam mit ihren Kollegen aus Island, Norwegen und der Schweiz eine Entschließung zum Internet, in der sie alle Staaten – und insbesondere diejenigen, die den größten Nutzen aus den neuen Technologien ziehen – auffordern, Maßnahmen zum Datenschutz zu verabschieden und umzusetzen (s. **Anlage 17**).

33 Aus meiner Dienststelle

33.1 Die Informationstechnik in meiner Dienststelle

Eine effiziente und wirtschaftliche Aufgabenerfüllung ist heute ohne IT-Einsatz unmöglich. Auch meine vielfältigen Kommunikationsbeziehungen zu den Behörden und Wirtschaftsunternehmen meines Zuständigkeitsbereiches machen eine sachgerechte, zeitgemäße IT-Ausstattung unerläßlich. Übrigens teilen mir bereits jetzt viele Bürger ihre Sorgen und Beschwerden „elektronisch“ – auch per E-Mail – mit. Ich bin daher ständig bemüht, die Ausstattung meiner Dienststelle mit IT- und TK-Systemen der Entwicklung anzupassen und voranzubringen.

In den vergangenen Jahren wurde die Ausstattung meiner Dienststelle mit informationstechnischen Geräten immer mehr verbessert. Bei einem Ausstattungsgrad von 93% verfügen alle Mitarbeiter, die es wollen, über einen PC mit einem Drucker. Der PC ist in einem Netzwerk (local area network; LAN) mit 5 Servern integriert, das ihm über den IVBB (s. o. Nr. 8.6) auch den Zugang zum „World Wide Web (WWW)“ des Internet eröffnet (s. Abb. 13).

Als Betriebssystem wird zum Teil noch Windows 3.1 der Firma Microsoft eingesetzt. Aus Gründen der IT-Sicherheit verfügen diese PC über keine Festplatte (discless station). Im Zuge der Modernisierung werden sie nach und nach durch Windows-NT-Workstations abgelöst. Bei diesen modernen PC mit Pentium-II-Prozessoren sorgen die Sicherheitsmechanismen des Betriebssystems für eine angemessene Datensicherheit, die durch zusätzliche Sicherheitsmaßnahmen unterstützt werden, wie z. B. ein Kartenleser in der PC-Tastatur, worüber sich der befugte Mitarbeiter gegenüber „seinem PC“ identifiziert.

Als Bürokommunikationssoftware wird bis zur flächendeckenden Ausstattung meiner Dienststelle mit NT-fähigen PC einheitlich das Büro-Software-Paket „MS-Office 4.2“ der Firma Microsoft eingesetzt. Neben Textverarbeitung (Winword 6.0), Tabellenkalkulation (Excel 5.0), Geschäftsgrafikprogramm (PowerPoint 4.0), steht auch die E-Mail (MS-Mail) zur Verfügung. Sie wird intensiv auch zur hausinternen Versendung dienstlicher Mitteilungen genutzt und beschleunigt den Informationsfluß erheblich. Desweiteren ermöglicht sie die Verbindung zu allen Dienststellen im IVBB und – über ein Gateway – den Zugang zur Internet-Mail. So sind meine Mitarbeiter und ich weltweit unter einer individuellen E-Mail-Kennung erreichbar. Die „Hausanschrift“ meiner Dienststelle ist **poststelle@bfd.bund400.de.**

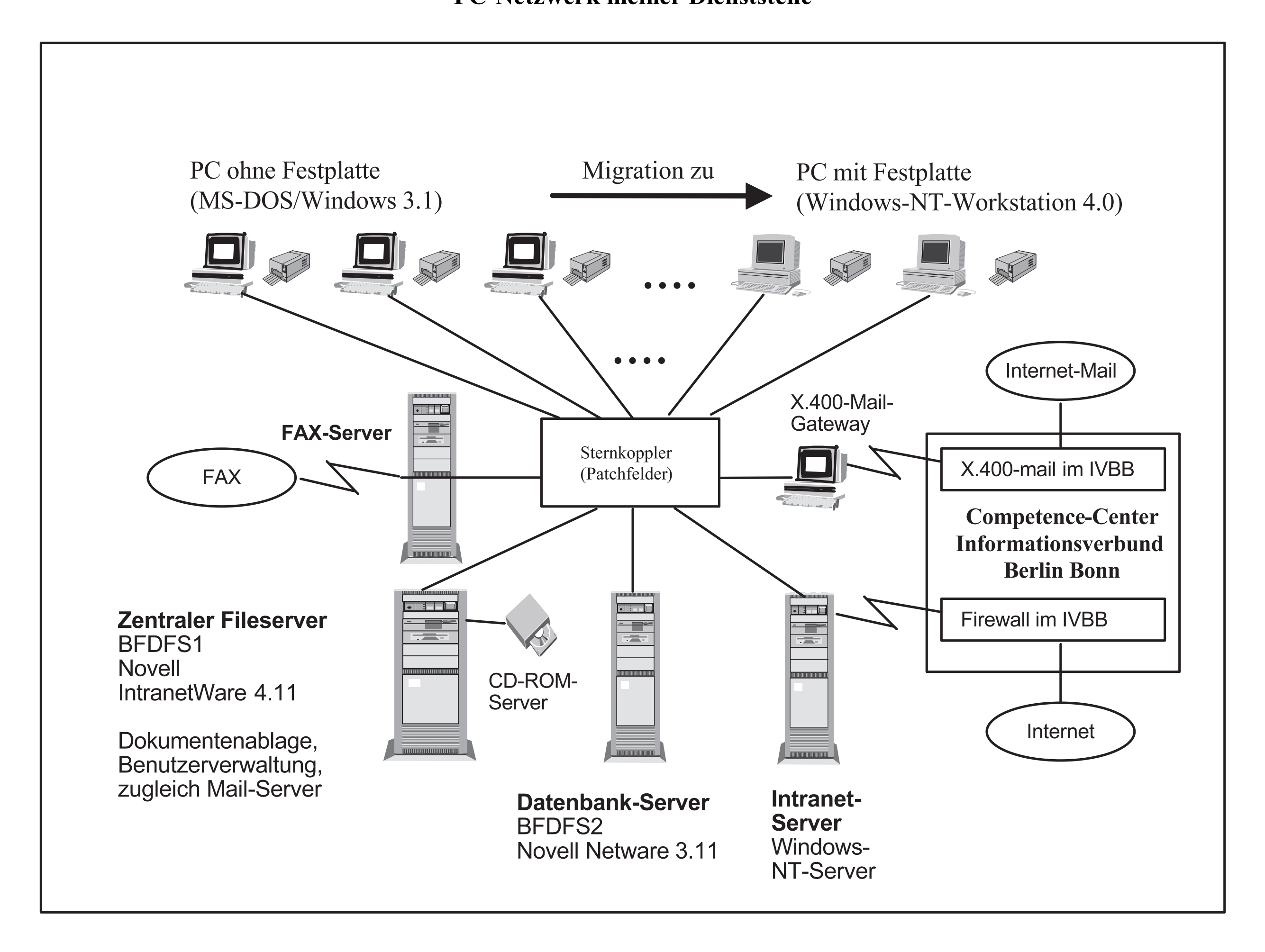
Alle PC sind sternförmig mit dem **zentralen Fileserver** verbunden. Die sternförmige Vernetzung hat sich aus der Sicht der IT-Sicherheit bewährt, da sich ein Fehler an einem PC dann nicht auf das ganze Netz auswirken kann. Der zentrale Fileserver mit dem Betriebssystem Novell IntranetWare verwaltet den Zugang zum PC-Netz und speichert die von den Nutzern erstellten und bearbeiteten Dokumente. Zusätzlich ist auf diesem Server das „Postoffice“ der Mail installiert.

Über einen weiteren **Gateway-Rechner** wird der Mail-Zugang zum IVBB hergestellt.

Zur Unterstützung der täglichen Arbeit ist am zentralen Fileserver ein **CD-ROM-Server** angeschlossen. In den 13 CD-ROM-Laufwerken werden jedem PC-Benutzer zentrale Informationssysteme zur Verfügung gestellt, wie z. B. die Gesetzessammlung „Schönfelder“ und „Satorius“ als CD-ROM-Fassung oder auch das „IT-Grundschutzhandbuch des Bundes“.

Abbildung 13 (zu Nr. 33.1)

PC-Netzwerk meiner Dienststelle



Der **Datenbank-Server** unterstützt mit einem elektronischen Schriftgutverwaltungssystem meine Registratur, wodurch die Verwaltung von Schriftstücken vereinfacht und beschleunigt wird. Der vierte Server stellt als **Intranet-Server** das hausinterne Informationssystem bereit.

Der **FAX-Server** ermöglicht das Versenden von Dokumenten vom PC aus.

33.2 Der Datenschutzbeauftragte jetzt auch im Internet – aber mit Sicherheit!

Seit Februar 1999 ist meine Dienststelle mit einem eigenem Angebot im Internet vertreten. Die Homepage meiner Dienstelle ist unter der „Internet-Adresse" **http://www.bfd.bund.de** erreichbar und umfaßt u. a. folgende Angebote, die ständig fortgeschrieben werden:

– Bürger und Datenschutz
– Wir über uns
– Aktuelles zum Datenschutz
– Informationsmaterial und
– Kontakte

(s. Abb. 14).

Da die Nutzung des Internet ein bekanntes Sicherheitsrisiko für die hausinternen PC-Netze darstellt, ist mein Angebot auf einem virtuellen Server beim Competence Center Informationsverbund Berlin-Bonn bei der Telekom AG (CCIVBB) abgelegt.

Das CCIVBB ist mit seiner zentralen Firewall für alle obersten Bundesbehörden die **1. Sicherheitsstufe** zum Internet.

In der **2. Stufe** der Netzsicherheit werden virtuelle Intranet-Server für das „Intranet des Bundes im IVBB" vorgehalten. Durch die zentrale Firewall geschützt, können so Informationsangebote für den behördeninternen Gebrauch vom Internet abgekoppelt und vor Zugriffen Dritter geschützt werden. Im Intranet des Bundes ist mein Haus für die IVBB-Dienststellen – insbesondere die obersten Bundesbehörden – unter der URL (Uniform Resource Locator) **http://www.bfd.ivbb.bund.de** erreichbar.

Da jede oberste Bundesbehörde einen eigenen Adressraum im Intranet des Bundes benutzt und eigene Schlüsselkreise für den geschützten Anschluß an das CCIVBB einsetzt, ist so eine Entkopplung der jeweiligen hausinternen Netze gegeben.

Abbildung 14 (zu Nr. 33.2)

Homepage des BfD



Abbildung 15 (zu Nr. 33.2)

Sicherheitsstufen für den BfD im Internet

Internet

Stufe 1: Zentrale Firewall des IVBB

Zentrale Firewall beim CC IVBB (Competence Center Informationsverbund Berlin/Bonn)

www.bfd.bund.de
Virtueller **Interne**t-Server des BfD

Virtuelle **Internet**-Server der obersten Bundesbehörden

Provider (CC IVBB)

Stufe 2: Sicherheit im Intranet des Bundes

www.bfd.ivbb.bund.de
Virtueller **Intranet**-Server des BfD im IVBB

Virtuelle **Intranet**-Server der obersten Bundesbehörden

Intranet des Bundes im IVBB

Verschlüsselte Anbindung mit eigenen Schlüsselkreisen

Stufe 3 : Hausinterne Sicherheit

Hausinternes Informationssystem
(Intranet-Server
Windows-NT-Server)

Internet-Gateway
Novell
IntranetWare 4.11

PC ohne Festplatte
Internet Explorer

PC mit Festplatte
Netscape-Browser

Dienststelle des BfD

Hausinterne PC-Netze

Oberste Bundesbehörden

In der **3. Sicherheitsstufe** entkoppelt ein Internet-Gateway-Rechner mein hausinternes PC-Netz vom Intranet des Bundes (s. Abb. 15).

34 Am Schluß noch einiges wichtige aus zurückliegenden Tätigkeitsberichte

1. Das Bundesausfuhramt und das Zollkriminalamt haben mittlerweile eine auf der Grundlage meiner Vorschläge erarbeitete **Vereinbarung über die Übermittlung von Ausfuhrdaten** (vgl. 15. TB Nr. 6.3) geschlossen und umgesetzt. Meine Kontrolle des Übermittlungsverfahrens im Jahr 1998 ergab, daß die Vereinbarung durch beide Behörden datenschutzgerecht umgesetzt wird.

2. Das BMVg hat die **Personalaktenverordnung** nach § 27 Wehrpflichtgesetz (BGBl. 1998 I S. 3169) inzwischen erlassen (vgl. 15. TB Nr. 35 unter 10.). Mit der Verordnung, bei deren Abstimmung ich beteiligt war, ist nunmehr ein erfreulicher datenschutzrechtlicher Standard auch für das Personalaktenrecht der **Wehrpflichtigen** erreicht worden.

3. Die geplante Neufassung des **Personenstandsgesetzes** (vgl. 16. TB Nr. 5.12) konnte im Berichtszeitraum noch nicht verwirklicht werden. Umfangreiche Stellungnahmen der Innenressorts der Länder sowie der Kirchen zu dem Entwurf des BMI machen weitere Beratungen auch in dieser Legislaturperiode erforderlich.

4. Im März 1996 hatte mir das BMI einen Referentenentwurf zur Änderung des **Bundeswahlgesetzes** übersandt (vgl. 16. TB Nr. 5.13), in dem meine langjährige Forderung berücksichtigt wurde, die Auslegung des Wählerverzeichnisses abzuschaffen. Leider wurde dieser Entwurf in der vergangenen Legislaturperiode nicht zur Beratung in das Parlament eingebracht. Ich hoffe, daß die geplante Änderung des Bundeswahlgesetzes nunmehr in Kürze erfolgt und damit die angestrebte datenschutzfreundliche Lösung umgesetzt wird.

5. In meinem 16. TB (Nr. 6.6) habe ich über den Entwurf eines **Zweiten Gesetzes zur Entlastung der Rechtspflege – Strafrechtlicher Bereich –** berichtet, der u. a. vorsah, die strafrechtliche Sanktionierung einer Verletzung der Vertraulichkeit des Wortes (§ 201 Abs. 1 und 2 StGB) in den Katalog der Privatklagedelikte gemäß § 374 Abs. 1 StPO aufzunehmen. Dieser weitgehenden Relativierung des strafrechtlichen Schutzes der vertraulichen Kommunikation bin ich entgegengetreten. Der Entwurf konnte in der abgelaufenen Legislaturperiode nicht mehr abschließend beraten werden. Sollte er in der 14. Legislaturperiode erneut eingebracht werden, werde ich mich dafür einsetzen, den Schutz der Vertraulichkeit des Wortes wie bisher zu erhalten und zu wahren.

6. Die in meinem 16. TB (Nr. 6.12) noch als Inhalt eines Referentenentwurfs beschriebenen Ergänzungen des **Bundesverfassungsgerichtsgesetzes** um – begrenzte – Regelungen über **Hörfunk- und Fernsehaufnahmen bei Verfahren vor dem Bundesverfassungsgericht** sowie über **Aktenauskunft und Akteneinsicht** sind inzwischen mit dem Gesetz zur Änderung des Bundesverfassungsgerichtsgesetzes und des Gesetzes über das Amtsgehalt der Mitglieder des Bundesverfassungsgerichts (BGBl. 1998 I S. 1823) in Kraft getreten. Die Praxis wird zeigen, ob die neuen Vorschriften, insbesondere über Hörfunk- und Fernsehaufnahmen, ausreichen, den Schutz des Persönlichkeitsrechts Betroffener in Verfahren vor dem Bundesverfassungsgericht zu gewährleisten.

7. **Aufbewahrungsbestimmungen und Dateiregelungen im Justizbereich,** über die ich in meinem 16. TB (Nr. 6.14) berichtet habe, sind aufgrund der Organisationszuständigkeit, aber auch wegen der Anzahl der dort anfallenden Akten vorrangig eine Angelegenheit der Länder. Einige Länder haben bereits Verwaltungsvorschriften mit inzwischen verkürzten Fristen, z. B. für den Bereich der ordentlichen Gerichtsbarkeit, erlassen oder arbeiten hieran. Das BMJ ist hinsichtlich der Bundesgerichte mit der Frage der Verkürzung von Aufbewahrungsfristen befaßt; zugleich prüft es in seinem Zuständigkeitsbereich, in welchem Umfang man eine gesetzliche Grundlage für die Aufbewahrung der Akten während des Laufs dieser Fristen benötigt. Zu welchem Ergebnis die Prüfung führen und wann sie abgeschlossen sein wird, läßt sich nach Auskunft des BMJ noch nicht absehen.

8. Im 16. TB (Nr. 7.4.1) hatte ich die uneinheitliche Praxis der Erstattung von **Kontrollmitteilungen der Hauptzollämter** an die Finanzämter kritisiert. Eine von mir erbetene Übersicht über die Verfahren, bei denen spontane und regelmäßige Kontrollmitteilungen aus Sicht der Finanzverwaltung unverzichtbar sind, und über die hierfür herangezogenen Rechtsgrundlagen hat mir das BMF leider nicht zur Verfügung gestellt. Während des Berichtszeitraums habe ich bei Beratungs- und Kontrollbesuchen von Hauptzollämtern aber auch keine weiteren Datenschutzverstöße durch unzulässige Kontrollmitteilungen festgestellt.

9. Ende November 1996 hatte mir das BMF den Entwurf einer **„Vorläufigen Dienstanweisung für den Einsatz des IT-Verfahrens AVS-APC bei den Vollstreckungsstellen der Hauptzollämter“** übersandt, der die von mir geforderten und seit 1992 vom BMF zugesagten Datenschutzregelungen enthalten sollte (vgl. 16. TB Nr. 7.5.2). Ich habe den Entwurf im Februar 1997 mit dem BMF erörtert, inhaltliche Änderungen und Ergänzungen angeregt und darum gebeten, die Dienstanweisung baldmöglichst zu erlassen. In der Stellungnahme der Bundesregierung vom 27. Februar 1998 zu meinem 16. TB hat das BMF hierzu ausgeführt, „daß eine überarbeitete Neufassung

des Entwurfs einer Dienstanweisung mit den erforderlichen Datenschutzregelungen derzeit in Bearbeitung ist und in Kürze fertiggestellt sein wird.“ Ein überarbeiteter Entwurf liegt mir seit März 1999 vor.

10. Meine Empfehlung, die Datenschutzregelungen in den Durchführungsbestimmungen zum **Vertrag mit der Russischen Föderation über die Zusammenarbeit und gegenseitige Unterstützung der Zollverwaltungen** zu ergänzen und zu präzisieren (vgl. 16. TB Nr. 7.9.2), ist erfreulicherweise vom BMF mit dem Verhandlungspartner umgesetzt worden. Die Bestimmungen enthalten neben einer Definition des Begriffs „personenbezogene Daten“ die von mir vorgeschlagene Löschungsverpflichtung und eine Klausel zur Gewährleistung eines angemessenen Schutzniveaus i.S. des Artikel 25 Abs. 1 EG-Datenschutzrichtlinie.

11. Nachdem das Bundesverwaltungsgericht die Angabe des Erläuterungstextes „Sozialleistung“ auf dem **Überweisungsträger** von Sozialhilfezahlungen als unzulässige **Offenbarung von Sozialdaten** qualifiziert hatte, hatte ich in meinem 16. TB (Nr. 19.5) über die Auswirkungen dieser Entscheidung für andere unbare Sozialleistungen in Geld berichtet. Offen gelassen hatte ich seinerzeit noch die Frage, ob die besonderen Verhältnisse der Rentenzahlung durch den **Postrentendienst** der Deutschen Post AG eine abweichende Bewertung für diese Sparte der gesetzliche Sozialversicherung rechtfertigen. Die Rentenzahlungen sind ein Massengeschäft. Monatlich erfolgen weit über 20 Millionen solcher Überweisungen durch die bundesweit acht Postrentendienstzentren. Um die bei einer solchen Fallzahl unvermeidlichen Rückfragen, Fehlleitungen, Rückforderungen und sonstigen unwägbaren Sonderfälle reibungslos bewältigen zu können, ist eine für alle Beteiligten am Zahlungsvorgang zweifelsfreie Identifizierbarkeit der Zahlungen erforderlich. Das gilt um so mehr, als im Bereich der gesetzlichen Rentenversicherung der einzelne Versicherte mehrere Renten aus verschiedenem Rechtsgrund parallel beziehen kann. Daß eine „Rente“ überwiesen wird, ergibt sich aber bereits aus dem üblichen Absender „Postrentendienst". Im Gegensatz dazu kann eine Anweisung z. B. einer Stadt, wie Sozialhilfe oder Grundsteuerrückzahlung, unterschiedliche Gründe haben. Was es ist, ergebe sich erst aus dem vom Bundesverwaltungsgericht für unzulässig erklärten Erläuterungstext. Auch die vom Bundesverwaltungsgericht angestellte Überlegung, aus der Tatsache einer Sozialhilfezahlung kann auf die wirtschaftlichen Verhältnisse des Empfängers rückgeschlossen werden, ist auf den Bezug einer gesetzlichen Rente nicht übertragbar. Angesichts der genannten Besonderheiten habe ich gegen die Angabe von **Rentenversicherungsnummer** und **Rentenart** auf dem Überweisungsträger des Postrentendienstes keine Bedenken.

12. Im 16. TB (Nr. 21.3) hatte ich darüber berichtet, daß ich meine früheren datenschutzrechtlichen Bedenken gegen eine Erhebung von Adressdaten für **Werbemaßnahmen der Krankenkassen** zurückgestellt habe. Mittlerweile hat das BMG mir zugestimmt, daß den Krankenkassen die Möglichkeit eröffnet werden sollte, sich und ihre Aktivitäten direkt potentiellen neuen Mitgliedern durch Informationsmaßnahmen und personenbezogene Werbung darzustellen und hat eine gesetzliche Klärung zur Zulässigkeit personenbezogener Werbemaßnahmen in Aussicht gestellt.

13. In meinem 16. TB (Nr. 26.2) habe ich berichtet, wegen der Art und Weise, wie die **Disziplinarbücher in der Bundeswehr** geführt werden, bleibe auch nach erfolgter Tilgung mit großer Wahrscheinlichkeit erkennbar, daß eine Disziplinarmaßnahme verhängt worden war. Dies widerspräche dem in der Wehrdisziplinarordnug verankerten Rehabilitierungsgedanken. Ich hatte dem BMVg deshalb empfohlen, das Verfahren zur Tilgung von Disziplinarmaßnahmen so zu ändern, daß ein Rückschluß auf eine früher verhängte Maßnahme trotz Löschung nicht mehr möglich sei.

    Das BMVg hat dazu dargelegt, daß die hier in Frage stehenden Karteiblätter der Disziplinarbücher aus sehr unterschiedlichen Gründen vernichtet und neu angelegt würden. So sei ein neues Karteiblatt allein schon dann anzulegen, wenn es beschädigt oder unleserlich geworden sei. Ein unmittelbarer Rückschluß auf gelöschte Disziplinareintragungen sei somit nicht möglich. Deshalb sehe es keinen zwingenden Grund, die Regelungen für das Führen der Disziplinarbücher zu ändern. Der Argumentation des BMVg konnte ich mich nicht verschließen.

14. In meinem 16. TB (Nr. 26.4) berichtete ich, daß Teilnehmer einer **Mahnwache vor einer Kaserne** auf Anordnung des Kasernenkommandanten **unrechtmäßig fotografiert** worden waren. Das dabei entstandene Filmmaterial war nicht sofort vernichtet worden, weil es als Beweismittel für ein vom Kasernenkommandanten angestrengtes Verfahren vor dem Wehrdienstsenat des Bundesverwaltungsgerichts bereitgehalten werden mußte. Das Verfahren ist mittlerweile rechtskräftig abgeschlossen. Das BMVg hat mir das Filmmaterial übergeben; es wurde in meinem Hause vernichtet.

15. In meinem 16. TB (Nr. 27) habe ich berichtet, daß das BMFSFJ aufgrund der Ermächtigung in § 36 Abs. 8 ZDG den Entwurf einer **Rechtsverordnung** vorgelegt hatte, der die Einzelheiten des Umgangs mit den **Personalakten Zivildienstpflichtiger** regelt. Im Abstimmungsverfahren mit den beteiligten Ressorts wurde allerdings deutlich, daß für einige vorgesehene Regelungen (z. B. zu den die Tauglichkeit betreffenden Unterlagen und über die Einbeziehung der Personalakten der Kriegsdienstverweigerer in die Rechtsverordnung) ergänzende gesetzliche Vorgaben fehlten.

Entsprechende Änderungen im Zivildienstgesetz und im Kriegsdienstverweigerungsgesetz waren in dem bisherigen Entwurf für ein Artikelgesetz zur Novellierung des BDSG vorgesehen. Nachdem die BDSG-Novelle allerdings in der 13. Legislaturperiode nicht mehr in den Bundestag eingebracht worden ist, hoffe ich, daß sie recht bald in der neuen Legislaturperiode verabschiedet wird. Dann wird auch – auf der Grundlage der Änderungen und Ergänzungen des Zivildienstgesetzes und des Kriegsdienstverweigerungsgesetzes – das Personalaktenrecht für den Zivildienst, wie zuvor schon für die Wehrpflichtigen, einen aus meiner Sicht begrüßenswerten Standard erreicht haben.

16. In meinem 16. TB (Nr. 35 unter 2) hatte ich berichtet, daß im BMJ ein datenschutzrechtlich notwendiger **Vorschlag zur Neuregelung des Grundbucheinsichtsrechts** zur Entscheidung anstehe. Nachdem die Angelegenheit dennoch längere Zeit nicht vorangekommen war, teilte mir das BMJ unter Hinweis auf die bestehenden Vorschriften auf meine Nachfrage mit, man habe wegen anderer Prioritäten noch nicht abschließend klären können, ob und gegebenenfalls in welchem Umfang eine Neuregelung des Grundbucheinsichtsrechts erforderlich und sinnvoll möglich sei. Auch in dem mittlerweile vom BMJ vorgelegten Entwurf für eine Vereinsregisterverordnung und zur Änderung anderer registerrechtlicher Vorschriften, in dem einige grundbuchrechtliche Bestimmungen, u. a. zur Protokollierung der Einsicht in das maschinell geführte Grundbuch, novelliert werden sollen, fehlen weitergehende Regelungen.

    Ich würde es begrüßen, wenn die Überlegungen des BMJ bald im Sinne einer befriedigenden Neuregelung der Grundbucheinsicht insgesamt abgeschlossen werden könnten und ein entsprechender Referentenentwurf auf den Weg gebracht würde. Dieser sollte beispielsweise neben der Frage der Protokollierung auch die vom Umfang her sachgerechte Beschränkung der Grundbucheinsicht und die zweckgebundene Verwendung der hierdurch erhaltenen Daten (vgl. 15. TB Nr. 4.7.1) behandeln.

17. Die von mir zuletzt in meinem 16. TB (Nr. 35 unter 3) angesprochene **2. Zwangsvollstreckungsnovelle** ist inzwischen verkündet (BGBl. 1997 I S. 3039) und am 1. Januar 1999 in Kraft getreten. Meinen Bedenken gegen den in dem Gesetzentwurf des Bundesrates als Regel vorgesehenen Erlaß eines einheitlichen Pfändungs- und Überweisungsbeschlusses auch bei einer Mehrzahl von Drittschuldnern wurde u. a. mit Blick auf die entsprechende bisherige Verfahrensweise nicht gefolgt. Die nunmehr geltende Ergänzung des § 829 Abs. 1 ZPO, die den einheitlichen Pfändungs- und Überweisungsbeschluß jetzt im Gesetz als Regel vorsieht, verweist immerhin ausdrücklich auch auf die schutzwürdigen Interessen der Drittschuldner, die ausnahmsweise Anlaß sein können, gesonderte Beschlüsse gegenüber jedem einzelnen Drittschuldner zu erlassen. Es kommt somit auf die Anwendung der Vorschrift in der Praxis an. Ich werde die Angelegenheit gegebenenfalls erneut aufgreifen, wenn die schutzwürdigen Interessen der beteiligten Drittschuldner hierbei nicht ausreichend gewahrt werden.

Dr. Joachim Jacob

Der Bundesbeauftragte für den Datenschutz

Anlage 1 (zu Nr. 1.11)

Hinweis für die Ausschüsse des Deutschen Bundestages

Nachfolgend habe ich dargestellt, welche Kapitel dieses Berichts für welchen Ausschuß von *besonderem Interesse* sein könnten:

Ausschuss	Kapitel
Ausschuß für Wahlprüfung, Immunität und Geschäftsordnung	3.1
Auswärtigen Ausschuß	2; 4; 32; 34 Nr. 10
Innenausschuß	2; 5; 6.1 bis 6.4; 6.6; 8.1 bis 8.10; 9.1; 9.2.2; 10.1.5; 10.3; 11 bis 18; 25.2.2; 25.3; 28.1.4; 28.2; 29.5.1; 30.1; 33.1 bis 33.2
Rechtsausschuß	5.7; 5.9.1; 6; 10.1 bis 10.1.5; 32; 34 Nr. 7, Nr. 16 und Nr. 17
Finanzausschuß	7; 9.2; 28.2; 34 Nrn. 8 bis 10
Haushaltsausschuß	3.2
Ausschuß für Wirtschaft und Technologie	8.1 bis 8.10; 10.1 bis 10.3; 29.7; 29.8
Ausschuß für Arbeit und Sozialordnung	7.7; 18.1; 19 bis 24
Verteidigungsausschuß	15; 26; 34 Nr. 2 und Nr. 14
Ausschuß für Familie, Senioren, Frauen und Jugend	27; 34 Nr. 15
Ausschuß für Gesundheit	9.1; 19; 21 bis 25
Ausschuß für Verkehr, Bau- und Wohnungswesen	28
Ausschuß für die Angelegenheiten der Europäischen Union	2; 10.1.4; 28.1.3; 28.1.5; 32

Anlage 2 (zu Nr. 1.10)

Übersicht über die durchgeführten Kontrollen, Beratungen und Informationsbesuche

Deutscher Bundestag
- Verwaltung

Bundeskanzleramt
- Bundesnachrichtendienst

Auswärtiges Amt
- Geheimschutzbeauftragter
- 1 Botschaft

Bundesministerium des Innern
- Statistisches Bundesamt
- Bundesamt für die Anerkennung ausländischer Flüchtlinge
  Zentrale Nürnberg und 2 Außenstellen
- Bundesbeauftragter für die Unterlagen des Staatssicherheitsdienstes der ehemaligen DDR
  2 Außenstellen
- Bundesverwaltungsamt
  Ausländerzentralregister
- Bundesgrenzschutz mit Grenzschutzdirektion
- ein Bahnpolizeiamt
- eine Bahnpolizeiwache
- Bundeskriminalamt
- Deutsche Verbindungsbeamte bei EUROPOL/EDS
- Bundesamt für Verfassungsschutz
- Bundeszentrale für politische Bildung
- Bundesdruckerei

Bundesministerium der Justiz
- Bundeszentralregister
- Deutsches Patentamt

Bundesministerium der Finanzen
- Bundesamt für Finanzen
- Zollkriminalamt
- 5 Oberfinanzdirektionen
- 1 Rechenzentrum der Bundesfinanzverwaltung
- 1 Bundesvermögensamt
- 8 Hauptzollämter
- 1 Zollamt
- 1 Zollfahndungszweigstelle

Bundesministerium für Arbeit und Soziales
- Bundesanstalt für Arbeit
- 8 Arbeitsämter
- Gesundheitsdatenarchiv Wismut bei der Bundesanstalt für Arbeitsschutz und Arbeitsmedizin

Bundesministerium der Verteidigung
- Militärischer Abschirmdienst
- 2 Bundeswehreinheiten (Heer, Luftwaffe)
- 3 Kreiswehrersatzämter
- 1 digitale Vermittlungsstelle

Bundesministerium für Familie, Senioren, Frauen und Jugend
- Bundesamt für den Zivildienst
- 5 Verwaltungsstellen Zivildienst
- 1 Zivildienstschule

Bundesministerium für Gesundheit

Bundesministerium für Verkehr, Bau- und Wohnungswesen
- Bundesamt für Güterverkehr
- Bundeseisenbahnvermögen
- Wasser- und Schiffahrtsdirektion Nord

Deutsche Post AG
- Generaldirektion
- zentrale Briefermittlungsstelle Marburg
- Nachsendeauftragszentrum München
- 3 Postagenturen
- 1 ePost-Station
- 1 Briefverteilungszentrum

Deutsche Telekom AG
- 4 Niederlassungen

Bundesversicherungsanstalt für Angestellte

Deutsches Rotes Kreuz – Suchdienst Hamburg

Berufsgenossenschaften und Krankenkassen

Hauptverband der gewerblichen Berufsgenossenschaften
Großhandels- und Lagerei – Berufsgenossenschaft
Berufsgenossenschaft für den Einzelhandel
Barmer Ersatzkasse – Zentrale Wuppertal und drei Außenstellen
Deutsche Angestellten Krankenkasse – zwei Außenstellen
Bahnbetriebskrankenkasse Zentrale Frankfurt und eine Außenstelle
SIEMENS – Betriebskrankenkasse

6 Telekommunikationsdienstunternehmen

Sonstige

Datenstelle der Rentenversicherungsträger beim VDR
eine Privatfirma als Auftragnehmer nach § 80 SGB X
Wirtschaftsunternehmen u.a. wegen Verfahren zur Sicherheitsüberprüfung

Anlage 3 (zu Nr. 1.10)

Übersicht über Beanstandungen nach § 25 BDSG

Bundeskanzleramt

- Verstoß des BND gegen § 20 SÜG wegen Volltextspeicherung des sog. Schlußberichts in einer Datei, die der Sicherheitsüberprüfung dient (s. Nr. 16.2)

Bundesministerium des Innern

- Verstoß des BKA gegen § 18 Abs. 2 Satz 2 BDSG wegen unterbliebener Errichtungsanordnung bezüglich AFIS und Verstoß gegen § 24 Abs. 4 Satz 2 Nr. 1 BDSG wegen unterbliebener Stellungnahme zu einem Prüfbericht über das System AFIS (s. Nr. 11.8)
- Verstoß des BAFl gegen § 9 sowie Anlage zu § 9 Satz 1 BDSG wegen Mängel im Bereich der Datensicherheit bei dem Personalaktengeheimnis unterliegenden Mitarbeiterdaten (s. Nr. 18.9.1).
- Verstoß des BAFl gegen § 24 Abs. 4 BDSG wegen mangelnder Unterstützung bei der Erfüllung meiner Aufgaben durch stets ausweichende und zum Teil irreführende Antworten auf meine Fragen zur Verhaltens- und Leitungskontrolle von Mitarbeitern (s. Nr. 18.2.1).
- Verstöße des BStU gegen § 19 Abs. 6 Satz 2 i.V.m. § 12 Abs. 4 Satz 3 StUG durch Einsichtnahme in nichtanonymisierte Unterlagen des ehemaligen MfS, gegen § 19 Abs. 7 Satz 4 i.V.m. § 12 Abs. 4 Satz 3 StUG durch Herausgabe nichtanonymisierter Kopien aus Unterlagen des ehemaligen MfS und gegen § 19 Abs. 1 StUG durch Herausgabe anonymisierter Kopien aus Unterlagen des ehemaligen MfS trotz zwischenzeitlichen Wegfalls des Verwendungszweckes (s. Nr. 5.9.2).

Bundesministerium der Finanzen

- Verstoß gegen die in § 36 Abs. 2 und 3 StVG festgelegten Beschränkungen für Abrufe von Daten über Kfz-Halter, Verstoß gegen die in § 14 Abs. 2 und 3 FRV festgelegten Verpflichtungen zur Protokollierung von ZEVIS-Abrufen und Verstoß gegen § 36 Abs. 5 Nr. 2 StVG durch das Unterlassen von zur Sicherung der Zulässigkeit von ZEVIS-Abrufen erforderlichen Kontrollen durch das Zollkriminalamt (s. Nr. 28.2).
- Verstoß gegen § 19 Abs. 1 BDSG in mehreren Fällen durch Verweigerung der Auskunft durch das Bundesamt für Finanzen gegenüber Betroffenen über von ihnen erteilte Freistellungsaufträge (s. Nr. 7.1)
- Festlegung gegenüber Ärzten, besuchte Patienten in steuerlichen Fahrtenbüchern genau zu bezeichnen, so daß sie deren Daten bei Nachprüfung durch das Finanzamt entgegen § 102 Abs. 1 Nr. 3c AO offenbaren und damit gegen § 203 Abs. 1 Nr. 1 StGB verstoßen müssen (s. Nr. 7.2).
- Verstoß einer Oberfinanzdirektion gegen §§ 4 Abs. 1, 12 Abs. 4 und 28 BDSG wegen der Abgabe von Schreiben sensiblen Inhaltes ohne Mitwirkung des Betroffenen (s. Nr. 18.10.1).

Bundesministerium für Verkehr, Bau- und Wohnungswesen

- Verstoß gegen §§ 15 und 16 BDSG durch unzulässige Übermittlung personenbezogener Daten an Träger öffentlicher Belange sowie an Verbände und Vereine im Rahmen eines Planfeststellungsverfahrens und Unterlassung angemessener Maßnahmen zur Folgenminderung durch die Wasser- und Schiffahrtsdirektion Nord (s. Nr. 28.3).
- Verstoß wegen unbefugter Offenbarung von Personaldaten (s. Nr. 18.10.2).
- Verstöße des Hauptpersonalrates beim Bundesministerium für Verkehr, Bau- und Wohnungswesen in Wahrnehmung von Personalratsangelegenheiten (s. Nr. 18.10.2)

Bundesministerium für Wirtschaft und Technologie sowie Vorstand der Deutschen Post AG

- Verstoß der Deutschen Post AG gegen § 2 Abs. 2 PDSV in Verbindung mit § 1 Satz 2 PDSV durch unzulässige Erhebung und Speicherung personenbezogener Daten über die näheren Umstände des Postverkehrs und Verstoß gegen § 18 Abs. 1 und § 9 BDSG durch Unterlassen angemessener organisatorischer und technischer Maßnahmen zur Sicherstellung des Datenschutzes (s. Nr. 29.8).

Bundesministerium der Verteidigung

- Verstoß gegen § 6 SÜG wegen Nichtgewährung rechtlichen Gehörs bei der Feststellung von Sicherheitsbedenken (s. Nr. 15.3).

Bundesanstalt für Arbeit

- Verstoß gegen §§ 67b Abs. 1, 67c Abs. 1 und 2 SGB X in Verbindung mit Runderlassen der Bundesanstalt wegen unzulässiger Aufbewahrung eines psychologischen Gutachtens (siehe Nr. 20.4).
- Verstöße gegen § 90 Abs. 1 BBG wegen Mängeln bei der Führung von Personalakten für Mitarbeiter und rechtswidriger Vorgaben zur Führung von Personalakten (s. Nr. 18.2.5).

Verwaltungs-Berufsgenossenschaft

- Verstoß gegen § 67a Abs. 1, 3 und 4 SGB X wegen nicht erforderlicher Datenerhebung und fehlender Hinweise auf die Rechtsposition des Betroffenen und einer dritten Person bei Einschaltung einer privaten Detektei (s. Nr. 23.7.2).
- Verstoß gegen § 200 Abs. 2 SGB VII i.V.m. § 76 Abs. 2 SGB X wegen Übermittlung medizinischer Daten gegen den ausdrücklichen Widerspruch eines

Versicherten und Nichtgewährung des Gutachterauswahlrechts (s. Nr. 23.4.4.1).

– Verstoß gegen § 200 Abs. 2 SGB VII wegen Mißachtung des Gutachtervorschlagsrechts und anschließender Entscheidung wegen mangelnder Mitwirkung (s. Nr. 23.4.4.2).

Berufsgenossenschaft der chemischen Industrie

– Verstoß gegen § 200 Abs. 2 SGB VII i.V.m. § 76 Abs. 2 SGB X wegen Nichtgewährung des Gutachterauswahlrechts und wegen fehlenden Hinweises auf ein Widerspruchsrecht bei der Übermittlung medizinischer Daten (s. Nr. 23.4.4.3).

Bahnbetriebskrankenkasse

– Verstöße gegen § 78 a SGB X wegen fehlender technischer und organisatorischer Vorgaben zum Schutz der Sozialdaten und gegen § 24 Abs. 4 BDSG wegen mangelnder Unterstützung bei der Erfüllung meiner Aufgaben (s. Nr. 21.4).

Anlage 4 (zu Nrn. 2.1.2.1, 9.1.1, 30.1)

Deutscher Bundestag
13. Wahlperiode

Drucksache 13/11168

23. 06. 99

Beschlußempfehlung und Bericht

des Innenausschusses (4. Ausschuß)

zu der Unterrichtung durch den Bundesbeauftragten für den Datenschutz – Drucksache 13/7500 –

Tätigkeitsbericht 1995 und 1996 des Bundesbeauftragten für den Datenschutz – 16. Tätigkeitsbericht –

A. Problem

Mit dem 16. Tätigkeitsbericht gibt der Bundesbeauftragte für den Datenschutz einen Überblick über die Schwerpunkte seiner Arbeit in den Jahren 1995 und 1996 sowie einen Ausblick auf anstehende wichtige Fragen. Die Unterrichtung durch den Bundesbeauftragten für den Datenschutz hat u.a. die EG-Datenschutzrichtlinien, Forderungen für den Datenschutz im privaten Sektor auf den Weg ins Jahr 2000, das Spannungsverhältnis „Großer Lauschangriff“ – Datenschutz, datenschutzrechtliche Regelungen im Strafverfahren, den Sozialdatenschutz sowie die Rechtstatsachenforschung zum Gegenstand.

B. Lösung

Annahme der anliegenden Beschlußempfehlung *).

Einstimmigkeit im Ausschuß

C. Alternativen

Keine

D. Kosten

Keine

*) Hinweis: Die Beschlußempfehlung wurde in der 244. Sitzung des Deutschen Bundestages am 24. Juni 1998 angenommen.

Beschlußempfehlung

Der Bundestag wolle beschließen:

I. Zum 16. Tätigkeitsbericht – 16. TB –

1. Der Deutsche Bundestag erwartet, daß die Bundesregierung im Anschluß an die Novellierung des Bundesdatenschutzgesetzes einen datenschutzrechtlichen Gesetzesvorschlag erarbeitet, der den neueren technischen Entwicklungen Rechnung trägt.

   Dies gilt besonders für Videoüberwachungen, deren Zulässigkeit an klare Voraussetzungen zu binden ist und die nur unter einschränkenden Bedingungen ohne Kenntnis der betroffenen Bürger erfolgen dürfen (16. TB, Nr. 31.1).

   Eine Regelung über den Einsatz von Chipkarten ist notwendig, damit die in diesem Rahmen erfolgende Datenverarbeitung einschließlich der Datenspeicherung auf der Chipkarte auf den unbedingt erforderlichen Umfang beschränkt wird, die Kartenherausgeber eine zweckfremde Nutzung der Chipkartendaten durch technisch-organisatorische Maßnahmen verhindern und jeder Chipkarteninhaber eine Möglichkeit hat, sich kostenlos und ohne großen sonstigen Aufwand über den Inhalt seiner Chipkarte zu informieren (16. TB, Nr. 9 und 31.1).

2. Der Deutsche Bundestag hat im Informations- und Kommunikationsdienste-Gesetz den Verantwortlichen zur Aufgabe gemacht, die Gestaltung und Auswahl technischer Einrichtungen für Teledienste an dem Ziel auszurichten, keine oder so wenige personenbezogene Daten wie möglich zu erheben, zu verarbeiten und zu nutzen.

   Der Deutsche Bundestag fordert die Bundesregierung auf, dieses Prinzip auch für andere Bereiche sowie in der allgemeinen Datenschutzgesetzgebung zu verfolgen (16. TB, Nr. 8.1).

3. Der Deutsche Bundestag unterstützt die Bemühungen der Bundesregierung, eine Lösung für den Konflikt zwischen dem Schutz für medizinische Daten über Patienten und dem Datenbedarf zu finden, insbesondere der epidemiologischen Forschung zu erarbeiten, wobei auch die Möglichkeit zu erwägen ist, den gesetzlich besonders betonten Schutz von Gesundheitsdaten für diese Daten z. B. durch ein Forschungsgeheimnis zu gewährleisten (16. TB, Nr. 25.1).

4. Die Bundesregierung wird aufgefordert, alsbald den Entwurf eines ZKA-Gesetzes vorzulegen, damit die Aufgaben und insbesondere Befugnisse des ZKA und der übrigen Zollfahndungsbehörden klar und präzise durch den Gesetzgeber geregelt werden können (16. TB, Nr. 13.5).

5. Der Deutsche Bundestag fordert die Bundesregierung auf, beim Bundesamt für Verfassungsschutz auf eine Änderung des Verwaltungshandels hinzuwirken, um sicherzustellen, daß unverzüglich eine rechtzeitige Löschung nicht mehr benötigter Daten erfolgt (16. TB, Nr. 14.1).

6. Der Deutsche Bundestag unterstützt die Bemühungen der Bundesregierung, bei der nächsten Volkszählung von einer Totalerhebung abzusehen. Der Deutsche Bundestag begrüßt die Überlegungen der Bundesregierung, eine stichtagbezogene Auswertung der Melderegister vorzunehmen (16. TB, Nr. 30.8).

7. Der Deutsche Bundestag nimmt zur Kenntnis, daß die Bundesregierung gegenwärtig die Vorschläge des Bundesbeauftragten für den Datenschutz für Änderungen der Abgabenordnung unter datenschutzrechtlichen Gesichtspunkten nicht übernimmt. Der Deutsche Bundestag erwartet jedoch, daß die Bundesregierung im Einzelfall datenschutzrechtliche Empfehlungen zur Abgabenordnung auch künftig sorgfältig prüft und erforderliche Änderungen aufgreift (16. TB, Nr. 7.1).

8. Der Deutsche Bundestag fordert die Bundesregierung auf, in der zu erlassenden Datenschutzverordnung nach § 89 Abs. 1 Telekommunikationsgesetz (TKG) („TDSV-neu“) Regelungen über Kunden, die keine Eintragung in elektronische Verzeichnisse wünschen, so zu gestalten, daß sie keine Negativkennzeichnung der Betroffenen darstellen (16. TB, Nr. 10.4.5).

9. Für Telekommunikationsunternehmen bestimmt das TKG, daß Telefonkunden nur mit ausdrücklicher Einwilligung in CD-ROM und andere elektronische Verzeichnisse aufgenommen werden dürfen. Diese Regelung wird in der Praxis dadurch unterlaufen, daß andere Unternehmen, die nicht dem TKG unterliegen, diese Verzeichnisse herausgeben. Der Deutsche Bundestag fordert die Bundesregierung auf, Regelungen zu treffen, die dem entgegenwirken (16. TB, Nr. 10.4.5).

II. Zum 15. Tätigkeitsbericht – 15. TB –

1. Der Deutsche Bundestag wiederholt die Aufforderung in Nummer 4 seines Beschlusses vom 11. Dezember 1997 und bittet die Bundesregierung, bereichsspezifische Regelungen zum Arbeitnehmerdatenschutz alsbald vorzulegen und unverzüglich einen Bericht über den Stand der bisherigen Bemühungen dem Rechtsausschuß, dem Innenausschuß und dem Ausschuß für Arbeit und Sozialordnung vorzulegen.

2. Der Deutsche Bundestag wiederholt die Aufforderung in Nummer 8 seines Beschlusses vom 11. Dezember 1997 und bittet die Bundesregierung, eine Gesetzesinitiative zu ergreifen, um beim Einsatz moderner Informationstechnik im Gesundheitswesen den gebotenen Schutz dieser Daten auch außerhalb von Arztpraxen und Krankenhäusern sicherzustellen. Der Deutsche Bundestag hält den Handlungsbedarf für gesetzliche Regelungen zur Nutzung von Gesundheitsdaten für gegeben und erwartet umgehend eine Initiative der Bundesregierung, nicht nur um eventuelle Fehlentwicklungen zu vermeiden, sondern auch um Entwicklungssicherheit und Akzeptanz zu fördern.

3. Der Deutsche Bundestag begrüßt das Vorhaben, bei den gesetzlichen Regelungen der Telefonüberwachung vertrauensbildende Maßnahmen durch weitere verfahrenssichemde Maßnahmen, wie Berichterstattung an den Deutschen Bundestag und Verbesserung des Verfahrens der richterlichen Anordnung, bis Ende des Jahres

1998 zu überprüfen und hierüber dem Deutschen Bundestag zu berichten.

4. Der Deutsche Bundestag bittet die Bundesregierung, die Frage nach den Wechselbeziehungen zwischen Zeugnisverweigerungsrechten und Beschlagnahme- bzw. Verwertungsverboten nicht nur in bezug auf die herkömmlichen Beschlagnahmegegenstände weiterzuverfolgen, sondern auch in bezug auf Inhalte und Verbindungsdaten der Telekommunikation zu prüfen und hierüber dem Rechtsausschuß und dem Innenausschuß des Deutschen Bundestages einen Bericht vorzulegen.

Bonn, den 23. Juni 1998

Der Innenausschuß

Anlage 5 (zu Nr. 2.1.2.2)

Die Beschlüsse der Abteilung Öffentliches Recht des 62. Deutschen Juristentages Bremen 1998

D. Abteilung Öffentliches Recht

Thema: Geben moderne Technologien und die europäische Integration Anlaß, Notwendigkeit und Grenzen des Schutzes personenbezogener Informationen neu zu bestimmen?

1. Die Erfordernisse der modernen Informationstechnologien und Informationsdienste sowie die EG-Datenschutzrichtlinie mit ihren vereinheitlichenden Schutzstandards geben Anlaß, Datenschutz und Informationsrecht gesetzlich neu zu regeln. Der Inhalt dieser Neuregelung wird maßgeblich durch die informationsfordernden, informationsermöglichenden und informationsbegrenzenden Gehalte des Grundgesetzes bestimmt.
   angenommen: 44:0:0

2. Bei der gebotenen Neuorientierung muß der Datenschutz als konstitutiver Teil einer umfassenden Informationsordnung begriffen werden, für die das – auf den Gedanken der Informationsgerechtigkeit ausgerichtete – Informationsrecht den rechtlichen Rahmen bildet.
   angenommen: 40:3:1

   Geboten ist eine Informationsordnung, die u.a. den Zugang zu Informationen und den Umgang mit Informationen insbesondere im Hinblick auf den Schutz personenbezogener Daten regelt.
   angenommen: 38:3:2

   Vergleichbar schutzbedürftige Informationen juristischer Personen (insbesondere Betriebs- und Geschäftsgeheimnisse) sind einzubeziehen.
   angenommen: 35:10:2

   Das Datenrecht ist als Datenverkehrsordnung auszugestalten.
   angenommen: 35:6:4

3. Das künftige Informationsrecht sollte einheitliche Schutzstandards anstreben.
   angenommen: 38:1:5

   Dies schließt Differenzierungen nach den Grundrechtspositionen der Informationshandelnden (z. B. Medienfreiheit, Wissenschaftsfreiheit, Glaubensfreiheit) bzw. nach spezifischen Sachstrukturen (z. B. Gesundheits- und Sozialrecht, Strafprozeßrecht) ein.
   angenommen: 35:0:10

4. Die Reformschritte sind zu einem umfassenden Informationsgesetzbuch zusammenzuführen. Zur Vorbereitung soll unverzüglich eine Kommission eingerichtet werden.
   angenommen: 36:0:10

5. Es empfiehlt sich, ein grundsätzlich einheitliches materielles Datenschutzrecht für den öffentlichen und den privaten Bereich zu schaffen, dessen innere Differenzierungen sich nach den Unterschieden in der Schutzbedürftigkeit unter Beachtung der Selbstbestimmung (Freiwilligkeit) und des Gefahrenpotentials zu richten haben. (Antrag Hamm)
   angenomen: 23:21:1

6. Der Verbreitung strafbarer und jugendgefährdender Informationen ist - unter Beachtung des Zensurverbotes - insbesondere durch gesetzlich geregelte technische Vorkehrungen entgegenzuwirken.
   angenommen: 44:1:1

7. Ein Eckpfeiler der Neuregelung sind technischer Selbstschutz und Selbstregulierungen (z. B. Datenschutz-Audit, Codes of conduct).
   angenommen: 42:1:2

   Voraussetzung ist die nachprüfbare Wirksamkeit derartiger Vorkehrungen.
   angenommen: 37:4:5

   Dies setzt die Unabhängigkeit der Kontrollinstanzen, einschließlich der internen Datenschutzbeauftragten, voraus (Antrag Jaspers)
   angenommen: 23:12:9

8. Die Verschlüsselung personenbezogener Daten soll erlaubt bleiben, bei besonderen Gefährdungslagen geboten werden.
   angenommen: 43:0:3

   a) Ein gesetzliches Hinterlegungsgebot ist nicht vorzusehen.
      angenommen: 37:5:4

   b) Ein gesetzliches Hinterlegungsgebot ist vorzusehen. (Antrag Pitschas)
      abgelehnt: 4:38:4

   c) Die Fortentwickung der Informationsgesellschaft verlangt danach, Prinzipien des Datenschutzes und der Sicherheit der Informationsverarbeitung zum integralen Bestandteil der Produkte, Dienstleistungen und Beratungen zu machen. (Antrag Büllesbach)
      angenommen: 40:1:4

      Elektronischer Handel kann nur sicher funktionieren, wenn die freie Benutzung von kryptographi-

schen Produkten und Dienstleistungen gewährleistet ist. (Antrag Büllesbach)

angenommen: 36:1:8

Eine Beschränkung des Gebrauchs von Verschlüsselungstechniken ist daher abzulehnen. (Antrag Büllesbach)

angenommen: 35:1:9

9. Das künftige Informationsrecht soll sich wirkungsorientiert u.a. an folgenden Leitlinien ausrichten: Datenvermeidung und Datensparsamkeit, Zweckbindung der Daten, Systemdatenschutz, klare Verantwortlichkeiten im Datenumgang, Anonymisierung und Pseudonymisierung personenbezogener Daten, Datensicherheit durch technische und organisatorische Vorkehrungen, Folgenausgleich.

   angenommen: 40:1:4

10. Wirksame Kontrolle ist Voraussetzung eines erfolgreichen Datenschutzes.

    angenommen: 46:0:0

    Eine wesentliche Bedeutung kommt hierbei den unabhängigen Datenschutzbeauftragten im öffentlichen und privaten Bereich zu.

    angenommen: 41:1:4

    Die Datenschutzkontrolle durch öffentliche Stellen soll weisungsfrei und verselbständigt durchgeführt werden.

    angenommen: 37:6:3

11. Grenzüberschreitende Informationsflüsse und internationale Vernetzungen machen verstärkte internationale Zusammenarbeit und Regelungen unerläßlich.

    angenommen: 46:0:0

Anlage 6 (zu Nrn. 6.3, 11.1, 11.7, 11.8, 11.10.2, 12.2, 13.2)

§ 34 Absatz 1 BKAG
Errichtungsanordnung*)

(1) Das Bundeskriminalamt hat für jede bei ihm zur Erfüllung seiner Aufgaben geführte automatisierte Datei mit personenbezogenen Daten in einer Errichtungsanordnung, die der Zustimmung des Bundesministeriums des Innern bedarf, festzulegen:

1. Bezeichnung der Datei,
2. Rechtsgrundlage und Zweck der Datei,
3. Personenkreis, über den Daten gespeichert werden,
4. Art der zu speichernden personenbezogenen Daten,
5. Arten der personenbezogenen Daten, die der Erschließung der Datei dienen,
6. Anlieferung oder Eingabe der zu speichernden Daten,
7. Voraussetzungen, unter denen in der Datei gespeicherte personenbezogene Daten an welche Empfänger und in welchem Verfahren übermittelt werden,
8. Prüffristen und Speicherungsdauer,
9. Protokollierung.

Der Bundesbeauftragte für den Datenschutz ist vor Erlaß einer Errichtungsanordnung zu hören.

*) als Beispiel für eine Regelung hierzu

Anlage 7 (zu Nr. 6.2)

Entschließung der 53. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 17./18. April 1997 zu: Beratungen zum StVÄG 1996

Die Datenschutzbeauftragten des Bundes und der Länder wenden sich entschieden gegen die Entwicklung, im Gesetzgebungsverfahren zu einem Strafverfahrensänderungsgesetz 1996, die Gewährleistung der informationellen Selbstbestimmung im Strafverfahren nicht nur nicht zu verbessern, sondern vielmehr bestehende Rechte sogar noch zu beschränken. Dies gilt insbesondere für den Beschluß des Bundesrates, der gravierende datenschutzrechtliche Verschlechterungen vorsieht.

Bereits der Gesetzentwurf der Bundesregierung wird in Teilbereichen den Vorgaben des Bundesverfassungsgerichts nicht gerecht und fällt teilweise hinter den bereits erreichten Standard der allgemeinen Datenschutzgesetze und anderer bereichsspezifischer Regelungen (wie z. B. dem Bundeszentralregistergesetz und den Polizeigesetzen der Länder) zurück.

Kritik erheben die Datenschutzbeauftragten des Bundes und der Länder insbesondere an folgenden Punkten:

– Die Voraussetzungen für Maßnahmen der Öffentlichkeitsfahndung sind nicht hinreichend bestimmt. So wird z. B. nicht angemessen zwischen Beschuldigten und Zeugen differenziert.

– Für Privatpersonen und Stellen, die nicht Verfahrensbeteiligte sind, wird als Voraussetzung zur Auskunfts- und Akteneinsicht lediglich ein vages „berechtigtes“ statt eines rechtlichen Interesses gefordert.

– Die Regelungen über Inhalt, Ausmaß und Umfang von Dateien und Informationssystemen mit personenbezogenen Daten bei Staatsanwaltschaften sind unzureichend. Das hat zur Folge, daß nahezu unbeschränkt Zentraldateien oder gemeinsame Dateien eingerichtet und Daten ohne Berücksichtigung der Begehungsweise und Schwere von Straftaten gespeichert werden können. Die Zugriffsmöglichkeiten der Strafverfolgungs- und Strafjustizbehörden auf diese Daten gehen zu weit. Darüber hinaus werden Standardmaßnahmen des technischen und organisatorischen Datenschutzes (z. B. Protokollierung, interne Zugriffsbeschränkungen etc.) weitgehend abgeschwächt.

Die Bedenken und Empfehlungen der Datenschutzbeauftragten des Bundes und der Länder fanden in den ersten Beratungen des Bundesrates zum Gesetzentwurf nahezu keinen Niederschlag.

Darüber hinaus hat der Bundesrat in seiner Stellungnahme weitergehende datenschutzrechtliche Verschlechterungen beschlossen, die vor allem die Entfernung mehrerer im Gesetzentwurf noch vorhandener Beschränkungen und verfahrensrechtlicher Sicherungen zum Schutz des Persönlichkeitsrechts und des Rechtes auf informationelle Selbstbestimmung der Betroffenen zum Inhalt haben.

Beispiele hierfür sind:

– Der Richtervorbehalt für die Anordnung der Öffentlichkeitsfahndung und der längerfristigen Observation soll gestrichen werden.

– Die Verwendungsbeschränkungen bei Daten, die mit besonderen Erhebungsmethoden nach dem Polizeirecht gewonnen wurden, sollen herausgenommen werden.

– Das Auskunfts- und Akteneinsichtsrecht auch für öffentliche Stellen soll erheblich erweitert werden.

– Detaillierte Regelungen für Fälle, in denen personenbezogene Daten von Amts wegen durch Strafverfolgungs- und Strafjustizbehörden an andere Stellen übermittelt werden dürfen, die im weitesten Sinne mit der Strafrechtspflege zu tun haben, sollen gestrichen werden.

– Das Verbot soll gestrichen werden, über die Grunddaten hinausgehende weitere Angaben nach Freispruch, endgültiger Verfahrenseinstellung oder unanfechtbarer Ablehnung der Eröffnung des Hauptverfahrens Daten in Dateien zu speichern.

– Speicherungs- und Löschungsfristen für personenbezogene Daten in Dateien sollen ersatzlos gestrichen werden.

– Kontrollverfahren für automatisierte Abrufverfahren sollen aufgehoben werden und die Verwendungsbeschränkungen für Protokolldaten sollen entfallen.

Die Datenschutzbeauftragten des Bundes und der Länder fordern die Bundesregierung und den Deutschen Bundestag auf, bei den anstehenden weiteren Beratungen des Gesetzentwurfes die vom Bundesrat empfohlenen datenschutzrechtlichen Verschlechterungen nicht zu übernehmen und die noch bestehenden datenschutzrechtlichen Mängel zu beseitigen.

Hingegen sollten Vorschläge des Bundesrates für Regelungen für den Einsatz von Lichtbildvorlagen und für die Datenverarbeitung zur Durchführung des Täter-Opfer-Ausgleichs aufgegriffen werden.

Anlage 8 (zu Nr. 6.3)

Entschließung der 53. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 17./18. April 1997 zu: Genetische Informationen in Datenbanken der Polizei für erkennungsdienstliche Zwecke

Immer häufiger wird bei der Verfolgung von Straftaten am Tatort oder beim Opfer festgestelltes, sog. biologisches Material als Spurenmaterial durch die Polizei sichergestellt, mittels DNA-Analyse untersucht und mit anderen DNA-Materialien verglichen. Die DNA-Analyse ist zur Standardmethode geworden, um die Herkunft von Spurenmaterial von bestimmten bekannten Personen (Verdächtigen, Opfern, unbeteiligten Dritten) oder die Identität mit anderem Spurenmaterial unbekannter Personen feststellen zu können.

Der Gesetzgeber hat zwar vor kurzem im Strafverfahrensänderungsgesetz – DNA-Analyse („Genetischer Fingerabdruck“) – die Voraussetzungen und Grenzen genetischer Untersuchungen im Strafverfahren geregelt. Eine Festlegung, ob und in welchen Grenzen die Speicherung und Nutzung der durch eine DNA-Analyse gewonnenen Untersuchungsergebnisse in Datenbanken der Polizei zu erkennungsdienstlichen Zwecken zulässig ist, enthält dieses Gesetz jedoch nicht.

Bezüglich des Aussagegehalts der gespeicherten Daten der Analyseergebnisse ist ein grundsätzlich neuer Aspekt zu berücksichtigen:

Die automatisiert gespeicherten Informationen aus DNA-Merkmalen, die zum Zweck der Identitätsfeststellung erstellt worden sind, ermöglichen derzeit tatsächlich zwar keine über die Identifizierung hinausgehenden Aussagen zur jeweiligen Person oder deren Erbgut. In Einzelfällen können die analysierten nicht codierenden persönlichkeitsneutralen DNA-Merkmale jedoch mit codierenden Merkmalen korrespondieren. In Anbetracht der weltweiten intensiven Forschung im Bereich der Genom-Analyse ist es nicht ausgeschlossen, daß künftig auch auf der Basis der Untersuchung von bisher als nicht codierend angesehenen Merkmalen konkrete Aussagen über genetische Dispositionen der betroffenen Personen mit inhaltlichem Informationswert getroffen werden können. Dieses Risiko ist deshalb nicht zu vernachlässigen, weil gegenwärtig weltweit mit erheblichem Aufwand die Entschlüsselung des gesamten menschlichen Genoms vorangetrieben wird.

Dieser Gefährdung kann dadurch begegnet werden, daß bei Bekanntwerden von Überschußinformationen durch die bisherigen Untersuchungsmethoden andere Untersuchungmethoden (Analyse eines anderen Genomabschnitts) verwendet werden, die keine Informationen über die genetische Disposition liefern. Derartige Ausweichstrategien können jedoch zur Folge haben, daß die mit anderen Methoden erlangten Untersuchungsergebnisse nicht mit bereits vorliegenden vergleichbar sind. Datenspeicherungen über verformelte Untersuchungsergebnisse könnten daher dazu führen, daß einmal verwendete Untersuchungsformen im Interesse der Vergleichbarkeit beibehalten werden, obwohl sie sich als problematisch herausgestellt haben und unproblematische Alternativen zur Verfügung stehen, z. B. durch Verschlüsselung problematischer Informationen.

In Anbetracht dieser Situation und angesichts der Tendenz, mittels der DNA-Analyse gewonnene Daten nicht nur in einem bestimmten Strafverfahren zu verwenden, sondern diese Daten in abrufbaren Datenbanken auch für andere Strafverfahren zugänglich zu machen, fordern die Datenschutzbeauftragten des Bundes und der Länder ergänzend zu §§ 81e und f StPO für die automatisierte Speicherung und Nutzung von DNA-Identitätsdaten eine spezielle gesetzliche Regelung in der Strafprozeßordnung, um das Persönlichkeitsrecht der Betroffenen zu schützen:

1. Es muß ein grundsätzliches Verbot der Verformelung und Speicherung solcher Analyseergebnisse statuiert werden, die inhaltliche Aussagen über Erbanlagen ermöglichen.

   Im Hinblick auf die nicht auszuschließende Möglichkeit künftiger Rückschlüsse auf genetische Dispositionen ist bereits jetzt ein striktes Nutzungsverbot für persönlichkeitsrelevante Erkenntnisse zu statuieren, die aus den gespeicherten Verformelungen der DNA resultieren.

2. Wenn zum Zweck des Abgleichs mit Daten aus anderen Verfahren (also zu erkennungsdienstlichen Zwekken) DNA-Informationen automatisiert gespeichert werden sollen (DNA-Datenbank mit der Funktion, die bei Fingerabdrücken die AFIS-Datenbank des BKA besitzt), müssen darüber hinaus folgende Regelungen geschaffen werden:

   – Nicht jede DNA-Analyse, die zum Zweck der Aufklärung einer konkreten Straftat erfolgt ist, darf in diese Datei aufgenommen werden. Die Speicherung von Verformelungen der DNA-Struktur in eine Datenbank darf nur dann erfolgen, wenn tatsächliche Anhaltspunkte dafür vorliegen, daß der Beschuldigte künftig strafrechtlich in Erscheinung treten wird und daß die Speicherung aufgrund einer Prognose unter Zugrundelegung des bisherigen Täterverhaltens die künftige Strafverfolgung fördern kann.

   – Eine Speicherung kommt insbesondere dann nicht in Betracht, wenn der Tatverdacht gegen den Beschuldigten ausgeräumt wurde. Bereits erfolgte Speicherungen sind zu löschen. Gleiches gilt für den Fall, daß die Anordnung der DNA-Untersuchung oder die Art und Weise ihrer Durchführung unzulässig war.

- Die Aufbewahrungsdauer von Verformelungen der DNA-Struktur ist konkret festzulegen (z. B. gestaffelt nach der Schwere des Tatvorwurfs).

3. Voraussetzung für Gen-Analysen muß in jedem Fall mindestens die richterliche Anordnung sein, unabhängig davon, ob die Daten in einem anhängigen Strafverfahren zum Zweck der Straftatenaufklärung, wie in § 81f Absatz 1 Satz 1 StPO normiert, oder ob sie zum Zweck der künftigen Strafverfolgung (also zu Zwecken des Erkennungsdienstes) benötigt werden.

4. Ein DNA-Screening von Personengruppen, deren Zusammensetzung nach abstrakt festgelegten Kriterien ohne konkreten Tatverdacht gegenüber einzelnen erfolgt, führt im Regelfall zur Erhebung von DNA-Daten zahlreicher völlig unbeteiligter und unschuldiger Bürger. Die Daten dieser Personen sind unmittelbar dann zu löschen, wenn sie für das Anlaßstrafverfahren nicht mehr erforderlich sind. Sie dürfen nicht in verfahrensübergreifenden DNA-Dateien gespeichert werden und auch nicht mit solchen Datenbeständen abgeglichen werden.

Anlage 9 (zu Nr. 2.1.1.1)

Entschließung der 54. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 23./24. Oktober 1997 zu: Novellierung des Bundesdatenschutzgesetzes und Modernisierung des Datenschutzrechts

Die fristgerechte Harmonisierung des Datenschutzes entsprechend den Vorgaben der europäischen Datenschutzrichtlinie vom 24. Oktober 1995 droht zu scheitern. Die von dieser Richtlinie gesetzte Dreijahresfrist wird heute in einem Jahr ablaufen. Eine gründliche Beratung im Deutschen Bundestag wird durch den baldigen Ablauf der Legislaturperiode in Frage gestellt.

Noch immer gibt es keinen Kabinettsbeschluß; die Bundesregierung hat bisher noch nicht einmal einen abgestimmten Referentenentwurf vorgelegt. Sie gefährdet dadurch die rechtzeitige Umsetzung der Richtlinie und riskiert ein Vertragsverletzungsverfahren vor dem Europäischen Gerichtshof.

Für die Entwicklung des Datenschutzes ist diese Lage höchst nachteilig:

– Verbesserungen des Datenschutzes der Bürger, z. B. durch genauere Information über die Verarbeitung ihrer Daten, verzögern sich;

– dem Datenschutzrecht droht Zersplitterung, weil den Ländern eine Orientierung für die Anpassung der Landesdatenschutzgesetze fehlt.

Die Datenschutzbeauftragten des Bundes und der Länder appellieren daher an die Bundesregierung, für eine fristgerechte Umsetzung der Richtlinie Sorge zu tragen.

Zur Harmonisierung des europäischen Datenschutzrechts empfehlen die Datenschutzbeauftragten der Bundesregierung und dem Gesetzgeber folgende Grundsatzentscheidungen:

– weitgehende Gleichbehandlung des öffentlichen und des privaten Bereichs bei gleichzeitiger Verbesserung der Datenschutzkontrolle, insbesondere durch generell anlaßunabhängige Kontrolle und durch die ausdrückliche Festlegung der völligen Unabhängigkeit der Aufsichtsbehörden und die Erweiterung ihrer Eingriffsbefugnisse;

– Bestellung weisungsfreier Datenschutzbeauftragter auch bei öffentlichen Stellen mit dem Recht, sich jederzeit an den Bundes- oder Landesbeauftragten für den Datenschutz zu wenden;

– Bürgerfreundlichkeit durch einfache und verständliche Formulierung des BDSG, z. B. durch einen einheitlichen Begriff der Verarbeitung personenbezogener Daten entsprechend der Richtlinie;

– Gewährleistung eines einheitlichen, hohen Datenschutzniveaus durch Beibehaltung der Funktion des BDSG und der Landesdatenschutzgesetze als Querschnittsgesetze sowie durch Vermeidung eines Gefälles zwischen den Bereichen, die der EG-Datenschutzrichtlinie unterfallen, und den übrigen Gebieten, deren Datenschutzregelungen nicht verschlechtert werden dürfen,

– Sonderregelungen für Presse und Rundfunk nur, soweit zur Sicherung der Meinungsfreiheit notwendig.

Als ebenso vordringlich betrachten die Datenschutzbeauftragten eine Anpassung der noch von der Großrechnertechnologie der siebziger Jahre bestimmten gesetzlichen Regelungen an die heutige Informationstechnologie und an die Verhältnisse der modernen Informationsgesellschaft. Dazu gehören insbesondere folgende Punkte:

– Verbindliche Grundsätze für die datenschutzfreundliche Gestaltung von Informationssystemen und -techniken, so zur Datensparsamkeit, zur Anonymisierung und Pseudonymisierung, zur Verschlüsselung und zur Risikoanalyse;

– mehr Transparenz für die Verbraucher und mehr Eigenständigkeit für die Anbieter durch Einführung eines Datenschutzaudits;

– Erweiterung des Schutzbereichs bei Bild- und Tonaufzeichnungen, Regelung der Video-Überwachung;

– Sonderregelungen für besonders empfindliche Bereiche, wie den Umgang mit Arbeitnehmerdaten, Gesundheitsdaten und Informationen aus gerichtlichen Verfahren;

– Einführung einer Vorabkontrolle für besonders risikoreiche Datenverarbeitung, namentlich bei Verarbeitung sensitiver Daten;

– Regelungen für Chipkarten-Anwendungen;

– Verstärkung des Schutzes gegenüber Adressenhandel und Direktmarketing, unter anderem auch mindestens durch die Festlegung von Hinweispflichten hinsichtlich der Möglichkeit des Widerspruchs; vorzuziehen ist in jedem Fall eine Einwilligungsregelung;

– Verstärkung des Schutzes gegenüber der Einholung von Selbstauskünften vor Abschluß von Miet-, Arbeits- und ähnlich existenzwichtigen Verträgen;

– Datenexport nach Inlandsgrundsätzen nur bei angemessenem Schutzniveau im Empfängerstaat; Festlegung, unter welchen Voraussetzungen ein Mitgliedstaat Daten, die er im Anwendungsbereich der Richtlinie (also nach Inlandsgrundsätzen) erhalten hat, außerhalb ihres Anwendungsbereichs verwenden darf;

– möglichst weitgehende Ersetzung der Anmeldung von Dateien bei der Aufsichtsbehörde durch Bestellung weisungsfreier Datenschutzbeauftragter; Beibehaltung

des internen Datenschutzbeauftragten auch bei Sicherheitsbehörden;

– Stärkung der Kontrollrechte des Bundesbeauftragten und der Landesbeauftragten für den Datenschutz durch uneingeschränkte Kontrollbefugnis bei der Verarbeitung personenbezogener Daten in Akten einschließlich solcher über Sicherheitsüberprüfungen.

Die Konferenz weist ferner auf die Rechtspflicht der Länder hin, ihr Datenschutzrecht ebenfalls der EG-Richtlinie fristgerecht anzupassen.

Anlage 10 (zu Nr. 6.5)

Entschließung der 54. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 23./24. Oktober 1997 zu: Informationelle Selbstbestimmung und Bild-Ton-Aufzeichnungen bei Vernehmungen im Strafverfahren

Überlegungen des Gesetzgebers und eine beginnende öffentliche Diskussion, moderne Dokumentationstechnik der Wahrheitsfindung und dem Zeugenschutz in gerichtlichen Verfahren nutzbar zu machen, liegen auch im Interesse des Datenschutzes. Dabei ist allerdings zu beachten, daß Bild-Ton-Aufzeichnungen von Vernehmungen im Strafverfahren einen erheblichen Eingriff in das Persönlichkeitsrecht darstellen. Sie spiegeln die unmittelbare Betroffenheit der Beschuldigten oder Zeugen in Mimik und Gestik umfassend wider. Zweck und Erforderlichkeit dieses Eingriffs bedürfen einer sorgfältigen Begründung durch den Gesetzgeber. Sie bildet den Maßstab, der über Möglichkeiten, Grenzen und Verfahren der Videotechnologie im Strafprozeß entscheidet. Erkennbar und nachvollziehbar sollte sein, daß der Gesetzgeber die Risiken des Einsatzes dieser Technologie, insbesondere die Verfügbarkeit der Aufzeichnungen nach den allgemeinen Vorschriften über die Beweisaufnahme bedacht und bewertet hat. Ferner sollte erkennbar und nachvollziehbar sein, daß Alternativen zur Videotechnologie, namentlich die Verwendung von Tonaufzeichnungen, in die Erwägungen des Gesetzgebers aufgenommen wurden.

Nach Auffassung der Datenschutzbeauftragten des Bundes und der Länder sollten die vorliegenden Gesetzentwürfe des Bundesrates (Drucksache 13/4983 vom 19. Juni 1996) sowie der Fraktionen der CDU/CSU und F.D.P. (Drucksache 13/7165 vom 11. März 1997) in einem umfassenderen Bedeutungs- und Funktionszusammenhang diskutiert werden. Zunehmend tritt das Anliegen der Praxis hervor, Bild-Ton-Aufzeichnungen auch mit anderer Zielsetzung zu verwerten:

Bild-Ton-Aufzeichnungen ermöglichen eine vollständige und authentische Dokumentation nicht nur des Inhalts, sondern auch der Entstehung und Begleitumstände einer Aussage. Die Beurteilung ihres Beweiswerts wird dadurch deutlich verbessert. Zugleich dient eine nur einmalige Vernehmung, die möglichst zeitnah zum Tatgeschehen durchgeführt und aufgezeichnet wird, der Wahrheitsfindung und erhöht die Qualität der gerichtsverwertbaren Daten („Vermeidung kognitiver Dissonanzen“). Ausgehend von diesen Überlegungen, hat der Gesetzgeber unter Einbeziehung von Erkenntnissen der Vernehmungspsychologie zu prüfen, ob und inwieweit eine wortgetreue Abfassung von Vernehmungsniederschriften ausreicht und eine Aufzeichnung der Aussage nur im Wort auf Tonband für die Zwecke des Strafverfahrens in ihrer Beweisqualität der Videotechnologie sogar überlegen ist.

Für Videoaufzeichnungen des Betroffenen, die zu seinem Schutz gefertigt werden sollen, ist dessen Einwilligung unverzichtbare Voraussetzung für die Zulässigkeit einer Bild-Ton-Aufzeichnung im Strafverfahren. Sofern der Betroffene nicht in der Lage ist, die Bedeutung und Tragweite einer Bild-Ton-Aufzeichnung und ihrer Verwendungsmöglichkeiten hinreichend zu beurteilen, hat der Gesetzgeber festzulegen, wer anstelle des Betroffenen die Einwilligung erteilen darf. Vor Abgabe der Einwilligungserklärung ist der Betroffene umfassend aufzuklären, insbesondere auch über alle zulässigen Arten der weiteren Verwertung und über die Möglichkeit des Widerrufs der Einwilligung für die Zukunft. Die Aufklärung ist zuverlässig zu dokumentieren. Entsprechendes gilt für die Herausgabe von Videoaufzeichnungen.

Die Datenschutzbeauftragten des Bundes und der Länder fordern wirksame Vorkehrungen zum Schutz des Persönlichkeitsrechts bei Verwendung von Bild-Ton-Aufzeichnungen im Strafverfahren. Unabhängig von der Frage, welche Zielsetzung mit Bild-Ton-Aufzeichnungen im Strafverfahren verfolgt werden soll, sind hierbei insbesondere folgende Gesichtspunkte von Bedeutung:

1. Es ist sicherzustellen, daß der Eindruck des Aussagegeschehens z. B. durch Zeitlupe, Zeitraffer, Einzelbildabfolge, Standbild und Zoom nicht gezielt verfremdet oder verzerrt wird.
2. Einsatz und Verwertung von Bild-Ton-Aufzeichnungen sind so zu regeln, daß gesetzliche Zeugnisverweigerungsrechte gewahrt bleiben. Insbesondere ist eine weitere Nutzung der Aufnahme, auch zum Zwecke des Vorhalts, ausgeschlossen, wenn sich ein Zeuge auf sein Zeugnisverweigerungsrecht beruft.
3. Vorbehaltlich des o.g. Einwilligungserfordernisses darf eine Übermittlung von Videoaufzeichnungen an Stellen außerhalb der Justiz, wenn überhaupt, nur in Ausnahmefällen erlaubt sein, da nur so ein wirksamer Schutz vor Mißbrauch, etwa durch kommerzielle Verwertung, gewährleistet werden kann. Soweit der Gesetzgeber aus Gründen eines fairen, rechtsstaatlichen Strafverfahrens die Weitergabe von Videokopien an Verfahrensbeteiligte zuläßt, müssen jedenfalls wirksame Vorkehrungen gegen Mißbrauch gewährleistet sein, z. B. sichtbare Signierung und strafbewehrte Regelungen über Zweckbindungen und Löschungsfristen.
4. Eine Verwertung der Aufzeichnungen im Rahmen eines anderen Strafverfahrens ist nur zulässig, soweit

sie auch für die Zwecke dieses anderen Verfahrens hätten angefertigt werden dürfen.

5. Soweit eine Verwertung in einem anderen gerichtlichen Verfahren – etwa zur Vermeidung erneuter Anhörung kindlicher Zeugen vor dem Familien- oder Vormundschaftsgericht – zugelassen werden sollte, sind in entsprechenden Ausnahmeregelungen präzise Voraussetzungen hierfür abschließend zu bestimmen und enge Verwendungsregelungen zu treffen.

6. Spätestens mit dem rechtskräftigen Abschluß des Strafverfahrens sind grundsätzlich die Aufzeichnungen unter Aufsicht der Staatsanwaltschaft zu vernichten. Der Betroffene ist davon zu benachrichtigen. Soweit der Gesetzgeber ausnahmsweise zur Wahrung vorrangiger Rechtsgüter eine längere Aufbewahrung der Aufzeichnungen zuläßt, müssen Voraussetzungen, Umfang und Fristen der weiteren Aufbewahrung klar und eng geregelt werden.

Anlage 11 (zu Nr. 8.5)

Entschließung der 54. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 23./24. Oktober 1997 zu: Erforderlichkeit datenschutzfreundlicher Technologien

Moderne Informations- und Telekommunikationstechnik (luK-Technik) gewinnt in allen Lebensbereichen zunehmende Bedeutung. Die Nutzer wenden diese Technik z. B. in Computernetzen, Chipkartensystemen oder elektronischen Medien in vielfältiger Weise an und hinterlassen dabei zumeist umfangreiche elektronische Spuren. Dabei fällt in der Regel eine Fülle von Einzeldaten an, die geeignet sind, persönliche Verhaltensprofile zu bilden.

Den Erfordernissen des Datenschutzes wird nicht in ausreichendem Maße Rechnung getragen, wenn sich der Schutz der Privatheit des einzelnen lediglich auf eine Beschränkung des Zugangs zu bereits erhobenen, gespeicherten und verarbeiteten personenbezogenen Daten reduziert. Daher ist es erforderlich, bereits vor der Erhebung und Speicherung die zu speichernde Datenmenge wesentlich zu reduzieren.

Datensparsamkeit bis hin zur Datenvermeidung, z. B. durch Nutzung von Anonymisierung und Pseudonymisierung personenbezogener Daten, spielen in den unterschiedlichen Anwendungsbereichen der IuK-Technik, wie elektronischen Zahlungsverfahren, Gesundheits- oder Verkehrswesen, bisher noch eine untergeordnete Rolle. Eine datenschutzfreundliche Technologie läßt sich aber nur dann wirksam realisieren, wenn das Bemühen um Datensparsamkeit die Entwicklung und den Betrieb von luK-Systemen ebenso stark beeinflußt wie die Forderung nach Datensicherheit.

Die Datenschutzbeauftragten des Bundes und der Länder wollen in Zusammenarbeit mit Herstellern und Anbietern auf datenschutzgerechte Lösungen hinarbeiten. Die dafür erforderlichen Techniken stehen weitgehend schon zur Verfügung. Moderne kryptographische Verfahren zur Verschlüsselung und Signatur ermöglichen die Anonymisierung oder Pseudonymisierung in vielen Fällen, ohne daß die Verbindlichkeit und Ordnungsmäßigkeit der Datenverarbeitung beeinträchtigt werden. Diese Möglichkeiten der modernen Datenschutztechnologie, die mit dem Begriff „Privacy enhancing technology (PET)“ eine Philosophie der Datensparsamkeit beschreibt und ein ganzes System technischer Maßnahmen umfaßt, sollten genutzt werden.

Vom Gesetzgeber erwarten die Datenschutzbeauftragten des Bundes und der Länder, daß er die Verwendung datenschutzfreundlicher Technologien durch Schaffung rechtlicher Rahmenbedingungen forciert. Sie begrüßen, daß sowohl der Mediendienste-Staatsvertrag der Länder als auch das Teledienstedatenschutzgesetz des Bundes bereits den Grundsatz der Datenvermeidung normieren. Der in den Datenschutzgesetzen des Bundes und der Länder festgeschriebene Grundsatz der Erforderlichkeit läßt sich in Zukunft insbesondere durch Berücksichtigung des Prinzips der Datensparsamkeit und der Verpflichtung zur Bereitstellung anonymer Nutzungsformen verwirklichen. Die Datenschutzbeauftragten des Bundes und der Länder bitten darüber hinaus die Bundesregierung, sich im europäischen Bereich dafür einzusetzen, daß die Förderung datenschutzfreundlicher Technologien entsprechend dem Vorschlag der Kommission in das 5. Rahmenprogramm „Forschung und Entwicklung“ aufgenommen wird.

Neben Anbietern von Tele- und Mediendiensten sollten auch die Hersteller und Anbieter von luK-Technik bei der Ausgestaltung und Auswahl technischer Einrichtungen dafür gewonnen werden, sich am Grundsatz der Datenvermeidung zu orientieren und auf eine konsequente Minimierung gespeicherter personenbezogener Daten achten.

Anlage 12 (zu Nr. 19.8)

Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 20. Oktober 1997 zu den Vorschlägen der Arbeitsgruppe der ASMK „Verbesserter Datenaustausch bei Sozialleistungen“

Mit dem von der ASMK-Arbeitsgruppe vorgeschlagenen erweiterten Datenaustausch bei Sozialleistungen wird die Bekämpfung von Leistungsmißbräuchen angestrebt. Soweit dieses Ziel der Arbeitsgruppe mit einer Veränderung der Strukturen der Verarbeitung personenbezogener Daten im Sozialleistungsbereich – insbesondere mit veränderten Verfahren der Datenerhebung – erreicht werden soll, muß der verfassungsrechtlich gewährleistete Grundsatz der Verhältnismäßigkeit beachtet werden.

Die gegenwärtigen Regelungen der Datenerhebung im Sozialleistungsbereich sehen unterschiedliche Verfahren der Datenerhebung vor, vor allem

– Datenerhebungen beim Betroffenen selbst

– Datenerhebungen bei Dritten mit Mitwirkung des Betroffenen

– Datenerhebungen bei Dritten ohne Mitwirkung des Betroffenen aus konkretem Anlaß

– Datenerhebungen bei Dritten ohne Mitwirkung des Betroffenen ohne konkreten Anlaß (Stichproben/Datenabgleich).

Diese Verfahren der Datenerhebung sind mit jeweils unterschiedlich schwerwiegenden Eingriffen in das Persönlichkeitsrecht der Betroffenen verbunden. So weiß z. B. bei einer Datenerhebung beim Betroffenen dieser, wer wann welche Daten zu welchem Zweck über ihn erhebt und Dritte erhalten keine Kenntnis von diesen Datenerhebungen. Im Gegensatz dazu wird bei einer Datenerhebung bei Dritten ohne Mitwirkung des Betroffenen dieser darüber im unklaren gelassen, wer wann welche Daten zu welchem Zweck über ihn erhebt und Dritten werden Daten über den Betroffenen zur Kenntnis gegeben (z. B. der Bank die Tatsache, daß der Betroffene Sozialhilfeempfänger ist).

Dieses System der Differenzierung des Verfahrens der Datenerhebung entspricht dem Grundsatz der Verhältnismäßigkeit. Ferner ist zu differenzieren, ob Daten aus dem Bereich der Sozialleistungsträger oder Daten außerhalb dieses Bereichs erhoben werden.

In dem Bericht der Arbeitsgruppe wird dieses System zum Teil aufgegeben. Es werden Verfahren der Datenerhebung vorgesehen, die schwerwiegend in die Rechte der Betroffenen eingreifen, ohne daß hinreichend geprüft und dargelegt wird, ob minder schwere Eingriffe in das Persönlichkeitsrecht zum Erfolg führen können. Die Datenschutzbeauftragten wenden sich nicht um jeden Preis gegen Erweiterungen des Datenaustauschs, gehen aber davon aus, daß pauschale und undifferenzierte Änderungen des gegenwärtigen Systems unterbleiben.

Datenabgleichsverfahren sollen nur in Frage kommen bei Anhaltspunkten für Mißbrauchsfälle in nennenswertem Umfang. Deshalb müssen etwaige neue Datenabgleichsverfahren hinsichtlich ihrer Wirkungen bewertet werden. Daher ist parallel zu ihrer Einführung die Implementierung einer Erfolgskontrolle für das jeweilige Abgleichsverfahren vorzusehen, die auch präventive Wirkungen erfaßt. Dies ermöglicht, Aufwand und Nutzen zueinander in das verfassungsmäßig gebotene Verhältnis zu setzen.

Soweit unter Beachtung dieser Prinzipien neue Kontrollinstrumente gegen den Leistungsmißbrauch tatsächlich erforderlich sind, muß für den Bürger die Transparenz der Datenflüsse sichergestellt werden. Diese Transparenz soll gewährleisten, daß der Bürger nicht zum bloßen Objekt von Datenerhebungen wird.

Bezugnehmend auf die bisherigen Äußerungen des BfD und von LfD bestehen gegen folgende Vorschläge im Bericht gravierende Bedenken:

1. Mitwirkung bei der Ahndung des Mißbrauchs (für alle Leistungsträger) und Verbesserungen für die Leistungsempfänger (zu D.II.10.1 und B.I) (S. 30 u. S. 2)

Die vorgeschlagenen Möglichkeiten von anlaßunabhängigen Mißbrauchskontrollen beinhalten keine Klarstellung der gegebenen Rechtslage, sondern stellen erhebliche Änderungen des bisherigen abgestuften Systems der Datenerhebung dar.

Die mit der Datenerhebung verbundene Offenlegung des Kontaktes bzw. einer Leistungsbeziehung zu einem Sozialleistungsträger stellt einen erheblichen Eingriff für den Betroffenen dar, u.a. da sie geeignet ist, seine Stellung in der Öffentlichkeit, z. B. seine Kreditwürdigkeit, wesentlich zu beeinträchtigen. Anfragen bei Dritten ohne Kenntnis des Betroffenen lassen diesen im unklaren, welche Daten wann an wen übermittelt wurden.

Derartige Datenerhebungen werden vom geltenden Recht deshalb mit Rücksicht auf das verfassungsrechtliche Verhältnismäßigkeitsprinzip nur in begrenzten und konkretisierten Ausnahmefällen zugelassen. Von dieser verfassungsrechtlich gebotenen Systematik würde die vorgeschlagene Neuregelung grundlegend abweichen. Die Datenschutzbeauftragten betonen bei dieser Gelegenheit, daß Datenerhebungen, die sowohl pauschal und undifferenziert sind, als auch ohne Anlaß erfolgen, abzulehnen sind.

Die Datenschutzbeauftragten weisen schließlich darauf hin, daß gegen eine Ausnutzung der technischen

Datenverarbeitungsmöglichkeiten zugunsten des Betroffenen (B. I des Berichts) nichts spricht, solange die Betroffenen davon informiert sind und soweit sie dem Verfahren zugestimmt haben.

2. Nachfrage beim Wohnsitzfinanzamt des Hilfesuchenden zu Schenkungen und Erbschaften (zu D.I.1.1) (S. 6)

Die Datenschutzbeauftragten teilen nicht die Auffassung, daß Stichproben nach der geltenden Rechtslage zu § 21 Abs. 4 SGB X möglich sind. § 21 Abs. 4 SGB X ist eine Auskunftsvorschrift für die Finanzbehörden, die über die Datenerhebungsbefugnis der Sozialleistungsträger nichts aussagt. Die Leistungsträger dürfen diese Auskünfte bei den Finanzbehörden als Dritten nur nach Maßgabe des § 67a SGB X einholen, soweit das erforderlich ist.: Diese Erforderlichkeit setzt Anhaltspunkte für Leistungsmißbrauch im Einzelfall voraus.

3. Auskunftspflicht der Banken und Lebensversicherungen (zu D.II.1.6) (S. 13)

Die Datenerhebung im Sozialbereich ist von einer möglichst weitgehenden Einbeziehung des Betroffenen gekennzeichnet. Der Vorschlag zur Einführung einer Auskunftspflicht geht auf dieses differenzierte System der Datenerhebungen im Sozialbereich überhaupt nicht ein.

Die Annahme in der Begründung des Vorschlags, ohne eine derartige Auskunftspflicht bestünden keine sachgerechten Ermittlungsmöglichkeiten, trifft nicht zu. Der Betroffene ist verpflichtet, Nachweise zu erbringen; dazu können auch Bankauskünfte gehören. Allerdings ist dem Betroffenen vorrangig Gelegenheit zu geben, solche Auskünfte selbst und ohne Angabe ihres Verwendungszwecks beizubringen. Nur soweit dennoch erforderlich, ist der Betroffene im Rahmen seiner Mitwirkungspflicht gehalten, sein Einverständnis in die Erteilung von Bankauskünften zu geben.

Die vorgeschlagene pauschale Auskunftsverpflichtung birgt deshalb die Gefahr in sich, daß dann generell ohne Mitwirkung des Betroffenen und ohne sein Einverständnis sofort an die Bank/Lebensversicherung herangetreten wird mit der Wirkung, daß der Betroffene desavouiert wird.

Die Datenschutzbeauftragten halten deshalb eine Klarstellung für dringend erforderlich, daß derartige unmittelbare Anfragen und Auskünfte erst in Betracht kommen, wenn die Ermittlungen unter Mitwirkung des Betroffenen zu keinem ausreichenden Ergebnis führen und Anhaltspunkte dafür bestehen, daß bei der fraglichen Bank/Lebensversicherung nicht angegebenes Vermögen vorhanden ist.

4. Akzeptanz des Datenaustausches (zu E.IV) (S. 36)

Datenabgleiche beinhalten eine Verarbeitung personenbezogener Daten, die nicht beliebig durchgeführt werden darf und anerkanntermaßen einer gesetzlichen Grundlage bedarf. Die im Papier der Arbeitsgruppe unter E.IV vertretene These, daß anlaßunabhängige Datenabgleiche keiner speziellen gesetzlichen Grundlage bedürften, trifft deshalb nicht zu.

Die Datenschutzbeauftragten wenden sich nicht gegen einzelne Veränderungen der Datenverarbeitung im Sozialleistungsbereich, soweit sie tatsächlich erforderlich und verhältnismäßig sind und die zuvor aufgezeigten Grundsätze beachtet werden. Die Datenschutzbeauftragten sind dazu gesprächsbereit.

Anlage 13 (zu Nr. 9.2)

Entschließung der 55. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 19./20. März 1998 zu: Datenschutzprobleme der Geldkarte

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder wiederholt ihre Forderung aus ihrer Entschließung vom 13.10.1995 nach einem anonymen elektronischen Zahlungsverfahren bei elektronischen Geldbörsen. Dies gilt insbesondere für die Geldkarte des deutschen Kreditwesens, bei der in kartenbezogenen „Schattenkonten“ der Evidenzzentralen nicht nur der Kaufbetrag und ein identifizierbarer Händlerschlüssel, sondern auch der Kaufzeitpunkt gespeichert werden. Mit diesen Daten können sämtliche mit der Geldkarte getätigten Kaufvorgänge jahrelang nachvollzogen werden, wenn die Daten mit den persönlichen Kundendaten zusammengeführt werden. Diese Geldkarte erfüllt nicht die Forderungen der Datenschutzbeauftragten.

Außerdem werden die Kundinnen und Kunden über diese „Schattenkonten“ noch nicht einmal informiert. Die Herausgeber solcher Karten bzw. die Kreditinstitute haben aber die Pflicht, ihre Kundinnen und Kunden über Art und Umfang der im Hintergrund laufenden Verarbeitungsvorgänge zu informieren.

Unabhängig davon müssen bei der Geldkarte des deutschen Kreditwesens sämtliche Umsatzdaten in den Evidenzzentralen und auch bei den Händlern nach Abschluß der Verrechnung (Clearing) gelöscht oder zumindest anonymisiert werden.

Die Datenschutzbeauftragten fordern die Kartenherausgeber und die Kreditwirtschaft erneut dazu auf, vorzugsweise kartengestützte Zahlungssysteme ohne personenbezogene Daten – sog. White Cards – anzubieten. Die Anwendung ist so zu gestalten, daß ein karten- und damit personenbezogenes Clearing nicht erfolgt.

Der Gesetzgeber bleibt aufgerufen sicherzustellen, daß auch in Zukunft die Möglichkeit besteht, im wirtschaftlichen Leben im gleichen Umfang wie bisher bei Bargeldzahlung anonym zu bleiben.

Anlage 14 (zu Nr. 2.1.2.2)

Entschließung der 56. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 5./6. Oktober 1998 zu: Dringlichkeit der Datenschutzmodernisierung

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder begrüßt und unterstützt grundsätzlich die vom 62. Deutschen Juristentag (DJT) im September 1998 in Bremen gefaßten Beschlüsse zum Umgang mit Informationen einschließlich personenbezogener Daten. Von den gesetzgebenden Körperschaften erhofft sich die Konferenz die Berücksichtigung dieser Beschlüsse bei der nunmehr dringend erforderlichen Umsetzung der EG-Datenschutzrichtlinie in Bundes- und Landesrecht.

Insbesondere betont die Konferenz folgende Punkte:

- Die materiellen Anforderungen des Datenschutzrechts sind angesichts der wachsenden Datenmacht in privater Hand auf hohem Niveau grundsätzlich einheitlich für den öffentlichen wie für den privaten Bereich zu gestalten.
- Die anlaßfreie Aufsicht für die Einhaltung des Datenschutzes im privaten Bereich muß in gleicher Weise unabhängig und weisungsfrei ausgestaltet werden wie die Datenschutzkontrolle bei öffentlichen Stellen.
- Die Rechte der Bürgerinnen und Bürger sind zu stärken; als Voraussetzung für die Ausübung des Rechts auf informationelle Selbstbestimmung der Betroffenen sind die Verpflichtungen zu ihrer Information, Aufklärung und ihren Wahlmöglichkeiten ohne faktische Zwänge auszuweiten.
- Ein modernisiertes Datenschutzrecht hat die Grundsätze der Datenvermeidung, des Datenschutzes durch Technik, der Zweckbindung der Daten und ihres Verwendungszusammenhangs in den Mittelpunkt zu stellen.
- Zur Sicherstellung vertraulicher und unverfälschter elektronischer Kommunikation ist die staatliche Förderung von Verschlüsselungsverfahren geboten, nicht eine Reglementierung der Kryptographie.

Anlage 15 (zu Nr. 6.2)

Entschließung der 56. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 5./6. Oktober 1998 zu: Fehlende bereichsspezifische Regelungen bei der Justiz

Derzeit werden in allen Bereichen der Justiz – bei Staatsanwaltschaften, Gerichten und Gerichtsvollziehern – im Zuge von Modernisierungsvorhaben umfassende Systeme der automatisierten Datenverarbeitung eingeführt mit der Folge, daß sensible personenbezogene Daten auch hier in viel stärkerem Maße verfügbar werden als bisher. Sogar die Beauftragung Privater mit der Verarbeitung sensibler Justizdaten wird erwogen. Gerade vor dem Hintergrund dieser vollkommen neuen Qualität der Datenverarbeitung in der Justiz wird deutlich, daß die Rechtsprechung des Bundesverfassungsgerichts zum sogenannten Übergangsbonus hier keine tragfähige Grundlage für Eingriffe in die informationelle Selbstbestimmung mehr darstellen kann. Vielmehr müssen die Entscheidungen des Gesetzgebers den Maßstab für die weitere technische Ausgestaltung der Datenverarbeitung innerhalb der Justiz bilden und nicht umgekehrt. Dabei ist nicht nur für formell ausreichende Rechtsgrundlagen Sorge zu tragen. Auch Fragen der Datensicherheit und der Ordnungsmäßigkeit der Datenverarbeitung bedürfen der Regelung.

Seit dem Volkszählungsurteil des Bundesverfassungsgerichts sind 15 Jahre vergangen. Dennoch werden ausgerechnet im Bereich der Justiz sensible personenbezogene Daten nach wie vor ohne die vom Bundesverfassungsgericht geforderten bereichsspezifischen gesetzlichen Grundlagen erhoben und verarbeitet.

Die Datenschutzbeauftragten des Bundes und der Länder bekräftigen deshalb im Anschluß an ihren Beschluß der 48. Konferenz vom 26./27. September 1994 in Potsdam ihre wiederholten Forderungen zu bereichsspezifischen Regelungen bei der Justiz.

Zwar hat der Gesetzgeber in der abgelaufenen Legislaturperiode zumindest Regelungen über Datenerhebung, -verarbeitung und -nutzung im Strafvollzug sowie über die Datenübermittlung von Amts wegen durch Gerichte und Staatsanwaltschaften an Gerichte, Behörden und sonstige öffentlichen Stellen geschaffen.

Trotzdem sind in wichtigen Bereichen gesetzliche Regelungen weiterhin überfällig. Ausreichende gesetzliche Regelungen fehlen vor allem für

- weite Bereiche der Datenverarbeitung im Strafverfahren, insbesondere in automatisierten Dateien

  namentlich die

  - Übermittlung von Strafverfahrensdaten an nicht am Strafverfahren beteiligte dritte Stellen;
  - Rechte der Betroffenen (nicht nur der Beschuldigten, sondern auch von Zeugen und sonstigen Personen, deren Daten gespeichert werden) in bezug auf Daten, die im Zusammenhang mit einem Strafverfahren gespeichert werden.
- Aufbewahrung von Akten, Karteien und sonstigen Unterlagen sowie die Dauer der Speicherung in automatisierten Dateien;
- Datenübermittlung zu wissenschaftlichen Zwecken;
- Datenverarbeitung in der Zwangsvollstreckung;
- Datenverarbeitung im Jugendstrafvollzug;
- Datenverarbeitung im Vollzug der Untersuchungshaft.

Der Gesetzgeber sollte daher in der kommenden Legislaturperiode zügig die notwendigen Novellierungen, für die zum Teil ja schon erhebliche Vorarbeiten geleistet worden sind, aufgreifen. Dabei ist nicht die jeweils geübte Praxis zu legalisieren, sondern es muß vorab unter datenschutzrechlichen Gesichtspunkten geprüft werden, welche Form der Datenerhebung und -verarbeitung in welchem Umfang erforderlich ist. Ferner hat der Gesetzgeber jeweils bereichsspezifisch zu prüfen, inwieweit Aufgaben der Justiz und damit verbundene Datenverarbeitungen Privaten übertragen werden dürfen.

Der Entwurf für ein „StVÄG 1996“ erfüllt diese Voraussetzungen nicht, im Gegenteil fällt er teilweise hinter den bereits erreichten Standard der allgemeinen Datenschutzgesetze und anderer bereichsspezifischer Regelungen (wie z. B. dem Bundeszentralregistergesetz und den Polizeigesetzen der Länder) zurück. Zu kritisieren sind vor allem:

- Mangelnde Bestimmtheit der Voraussetzungen für Maßnahmen der Öffentlichkeitsfahndung;
- Unangemessen weite Auskunfts- und Akteneinsichtsmöglichkeiten für nicht Verfahrensbeteiligte;
- Unzureichende Regelungen über Inhalt, Ausmaß und Umfang von staatsanwaltschaftlichen Dateien und Informationssystemen.

Die Datenschutzbeauftragten halten es deshalb zum Schutz des Rechts des Einzelnen auf informationelle Selbstbestimmung für geboten, wegen der mit der Datenerhebung, Verarbeitung und Nutzung verbundenen Rechtseingriffe unverzüglich in der neuen Legislaturperiode bereichsspezifische Regelungen der materiellen Voraussetzungen sowie der organisatorischen und verfahrensrechtlichen Vorkehrungen zu schaffen, welche der Gefahr einer Verletzung des Persönlichkeitsrechtes der Bürgerinnen und Bürger entgegenwirken.

Anlage 16 (zu Nr. 7.1)

Entschließung der 56. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 5./6. Oktober 1998 zu: Verweigerung der Auskunft durch das Bundesamt für Finanzen auf Anfragen Betroffener über ihre Freistellungsaufträge

Die Datenschutzbeauftragten des Bundes und der Länder betonen das Recht der Bürgerinnen und Bürger auf Auskunft über ihre Daten auch gegenüber der Finanzverwaltung (§ 19 BDSG). Die Betroffenen haben Anspruch, von dem Bundesamt für Finanzen Auskunft über die Freistellungsaufträge zu erhalten, die sie ihrer Bank im Zusammenhang mit dem steuerlichen Abzug von Zinsen erteilt haben.

Der Bundesbeauftragte für den Datenschutz hat die Verweigerung der Auskünfte gegenüber dem Bundesministerium der Finanzen beanstandet und dieses aufgefordert, den entsprechenden Erlaß an das Bundesamt aufzuheben. Bisher hat das Ministerium in der Sache allerdings nicht eingelenkt.

Für die Betroffenen ergibt sich hierdurch ein unhaltbarer Zustand. Ihnen wird die Auskunft zu Unrecht vorenthalten.

Die Datenschutzbeauftragten der Länder unterstützen mit Nachdruck die Forderung des Bundesbeauftragten für den Datenschutz gegenüber dem Bundesministerium der Finanzen, seinen Erlaß an das Bundesamt für Finanzen aufzuheben und dieses anzuweisen, dem Auskunftsanspruch der Auftraggeber von Freistellungsaufträgen nachzukommen.

Anlage 17 (zu Nr. 32.4)

Entschließung der Datenschutzbeauftragten der Mitgliedstaaten der Europäischen Union sowie derjenigen Islands, Norwegens und der Schweiz zum Internet

Die unabhängigen Datenschutzbehörden der Europäischen Union zusammen mit denjenigen von Island, Norwegen und der Schweiz, die sich im Anschluß an die 20. Internationalen Konferenz in Santiago de Compostela am 16. und 17. September 1998 getroffen haben,

sind überzeugt, daß das Internet als ein Mittel dienen kann, die Demokratie zu stärken, indem es den Bürgern erlaubt, besser an öffentlichen Debatten teilzunehmen, und indem es öffentlichen Angelegenheiten höhere Publizität verschafft.

Sie machen darauf aufmerksam,

– daß der Gebrauch eines Mittels wie des Internets zur Verbreitung und Sammlung von Informationen und die Folgen, die dies für die Grundwerte hat, die Anerkennung der Notwendigkeit von Garantien erfordert und

– daß derartige Garantien international geschaffen werden müssen, ohne daß damit Hindernisse für die Meinungsfreiheit und das Recht auf Information errichtet werden.

Sie sind der Ansicht, daß auf der Basis der Grundsätze des Schutzes personenbezogener Daten, die in vielen Staaten bereits anerkannt sind und die auch für das Internet gelten, alle Staaten, und insbesondere diejenigen, in denen die Nutzung der neuen Technologien am weitesten verbreitet ist, Maßnahmen zum Schutz personenbezogener Daten ergreifen und verstärken und eine internationale Kooperation fördern müssen, die auf den weltweit anerkannten Werten beruhen und die sicherstellen, daß die steigende Nutzung des Internets keine Folgen hervorbringt, die mit dem Schutz personenbezogener Daten und der Persönlichkeitsrechte nicht vereinbar sind.

Sie weisen insbesondere darauf hin,

– daß Daten, die dafür mißbraucht werden können, Personen Gefahren auszusetzen oder sie herabzusetzen, auf dem Internet nicht in einer Weise verbreitet werden dürfen, die einen solchen Mißbrauch ermöglicht,

– daß effektive rechtliche und technische Maßnahmen entwickelt werden sollten, die es den betroffenen Personen ermöglichen, die Nutzung ihrer personenbezogenen Daten selbst zu bestimmen und zu kontrollieren,

– daß effektive Maßnahmen ergriffen werden sollten, um die Übereinstimmung mit den Prinzipien des Datenschutzes sicherzustellen durch alle Beteiligten, die verantwortlich für die Verbreitung oder Sammlung personenbezogener Daten im Internet sind oder die technische Infrastruktur des Internets zur Verfügung stellen.

Anlage 18 (zu Nr. 2.2.1)

Datenschutzgruppe nach Artikel 29 der EG-Datenschutzrichtlinie

Von der Arbeitsgruppe angenommene Dokumente

WP 1 (5012/97)	Empfehlung 1/97 Datenschutzrecht und Medien Angenommen am 25. Februar 1997
WP 2 (5023/97)	Stellungnahme 1/97 zu kanadischen Initiativen für eine Standardisierung im Bereich des Schutzes der Privatsphäre Angenommen am 29. Mai 1997
WP 3 (5025/97)	Erster Jahresbericht Angenommen am 25. Juni 1997
WP 4 (5020/97)	Erste Leitlinien für die Übermittlung personenbezogener Daten in Drittländer –Mögliche Ansätze für eine Bewertung der Angemessenheit Angenommen am 26. Juni 1997
WP 5 (5060/97)	Empfehlung 2/97 Bericht und Leitfaden der internationalen Arbeitsgruppe über Datenschutz im Bereich Telekommunikation („Budapest –Berlin Memorandum on Data Protection and Privacy on the Internet“) Angenommen am 3. Dezember 1997
WP 6 (5022/97)	Empfehlung 3/97 Anonymität im Internet Angenommen am 3. Dezember 1997
WP 7 (5057/97)	Arbeitsunterlage: Beurteilung der Selbstkontrolle der Wirtschaft: Wann ist sie ein sinnvoller Beitrag zum Niveau des Datenschutzes in einem Drittland? Angenommen am 14. Januar 1998
WP 8 (5027/97)	Arbeitsunterlage: Meldung Angenommen am 3. Dezember 1997
WP 9 (5005/98)	Arbeitsunterlage: Erste Überlegungen zur Verwendung vertraglicher Bestimmungen im Rahmen der Übermittlungen personenbezogener Daten an Drittländer Angenommen am 22. April 1998
WP 10 (5009/98)	Empfehlung 1/98 zu computergesteuerten Buchungssystemen von Luftfahrtunternehmen (CRS) Angenommen am 28. April 1998
WP 11 (5032/98)	Stellungnahme 1/98 „Platform for Privacy Preferences (P3P)“ und „Open Profiling Standard (OPS)“ Angenommen am 16. Juni 1998
WP 12 (5025/98)	Übermittlungen personenbezogener Daten an Drittländer: Anwendung von Artikel 25 und 26 der Datenschutzrichtlinie der EU Angenommen am 24. Juli 1998
WP 13 (5004/98)	Künftige Arbeit im Hinblick auf Verhaltensregeln: Arbeitsunterlage über das Verfahren für die Prüfung der Verhaltensregeln der Gemeinschaft durch die Arbeitsgruppe Angenommen am 10. September 1998
WP 14 (5047/98)	Zweiter Jahresbericht Angenommen am 30. November 1998
WP 15 (5092/98)	Stellungnahme 1/99 zum Stand des Datenschutzes in den Vereinigten Staaten und zu den derzeitigen Verhandlungen zwischen der Europäischen Kommission und der amerikanischen Regierung Angenommen am 26. Januar 1999

Die genannten Papiere können unter folgender Internetadresse bezogen werden:

http://www.europa.eu.int/comm/dg15

Anlage 19 (zu Nr. 2.1.1.2)

Der Bundesbeauftragte für den Datenschutz

Geschäftszeichen (bei Antwort bitte angeben)
I – 101/17

☎ (02 28)
8 19 95 –

Datum
30. Dezember 1998

Der Bundesbeauftragte für den Datenschutz, Postf. 20 01 12, 53131 Bonn

An die
obersten Bundesbehörden

lt. Verteiler

Betr.: **Umsetzung der europäischen Datenschutzrichtlinie 95/46/EG vom 24. Oktober 1995;**
hier: Direktwirkung

Anlg.: – 1 – (Text der Richtlinie 95/46/EG)

Nach dem Ablauf der dreijährigen Umsetzungsfrist für die europäische Datenschutzrichtlinie 95/46/EG am 24. Oktober 1998 sind die Grundsätze der ständigen Rechtsprechung des Europäischen Gerichtshofes (EuGH) zur unmittelbaren Anwendung (Direktwirkung) nicht rechtzeitig umgesetzter Richtlinien zu beachten.

Voraussetzung für die Direktwirkung einer Richtlinie ist, daß sie

(1) dem einzelnen ein hinreichend bestimmtes und unbedingtes (selbstexekutives) Recht

(2) im Verhältnis gegenüber dem Staat gewährt.

Folgende Fälle der Direktwirkung sind von Bedeutung:

1. Zulässigkeit

Artikel 8 (Verarbeitung besonderer Kategorien personenbezogener Daten)

Zu beachten ist das grundsätzliche Verarbeitungsverbot, soweit nicht das geltende Recht im Einklang mit der Richtlinie (Artikel 8 Abs. 1 bis 3 und 5) eine Verarbeitung erlaubt. Dies bedeutet, daß die Erlaubnistatbestände des BDSG teilweise keine Anwendung finden.

So dürfen Gesundheitsdaten etwa außerhalb des Anwendungsbereiches des angemessene Garantien bietenden Sozialversicherungsrechts (vgl. Artikel 8 Abs. 2b)) und außer durch ärztliches Personal (vgl. Artikel 8 Abs. 3) ohne Einwilligung des Betroffenen nicht mehr verarbeitet werden. Dem ist beispielsweise im Rahmen des Dienst- und Arbeitsrecht Rechnung zu tragen.

2. Rechte

– Artikel 14 Abs. 1a) i.V.m. Artikel 7e) und f) (Widerspruch der betroffenen Person)

Die datenverarbeitenden Stellen haben eingehende Widersprüche auf ihre Begründetheit zu prüfen und sie entsprechend zu berücksichtigen.

– Artikel 10c) und Artikel 11 Abs. 1c) (Information des Betroffenen)

Unter den von der Richtlinie bestimmten Voraussetzungen sind die dort genannten weiteren Informationen zu geben.

Sofern sie dem Betroffenen noch nicht vorliegen, erhält er weitere Informationen, beispielsweise betreffend

= die Empfänger oder Kategorien der Empfänger der Daten,

= das Bestehen von Auskunfts- und Berichtigungsrechten bezüglich sie betreffender Daten,

= die Frage, ob die Beantwortung der Fragen obligatorisch oder freiwillig ist, sowie mögliche Folgen einer unterlassenen Beantwortung (Artikel 10),

= die Datenkategorien, die verarbeitet werden (Artikel 11).

– Artikel 13 (Ausnahmen und Einschränkungen)

  Eine Auskunft an den Betroffenen darf nur unter den in der Richtlinie bestimmten Voraussetzungen (Artikel 13) verweigert werden: Darüber hinaus sind die entsprechenden Regelungen §§ 19 Abs. 4 und 34 Abs. 4 BDSG nicht mehr anwendbar.

– Artikel 13 Abs. 1 führt unter a) bis g) die folgenden Fälle auf:

  a) Sicherheit des Staates,
  b) Landesverteidigung,
  c) öffentliche Sicherheit,
  d) Strafverfolgung etc.,
  e) Wirtschafts- und Finanzinteressen eines Mitgliedstaates oder der Europäischen Union
  f) Ausübung öffentlicher Gewalt i.V.m. c), d) und e),
  g) den Schutz der betroffenen Person und der Rechte und Freiheiten anderer Personen.

3. Anwendungsbereich

Artikel 2, 3, 9 (Begriffsbestimmungen, Anwendungsbereich, Verarbeitung personenbezogener Daten und Meinungsfreiheit)

Die Richtlinie geht von einem umfassenden Verarbeitungs- und Dateibegriff aus. Die Rechte des einzelnen gelten dementsprechend für einen erweiterten Anwendungsbereich. Im BDSG vorgesehene Einschränkungen und Ausnahmen (z.B. für vorübergehende und interne Dateien nach § 1 Abs. 3 und für Medien nach § 41 Abs. 1 BDSG) sind nicht mehr bzw. nur noch nach Maßgabe der Richtlinie anzuwenden.

Anlage 20 (zu Nr. 8.12)

Der Bundesbeauftragte für den Datenschutz

Geschäftszeichen (bei Antwort bitte angeben)	☎ (02 28)	Datum
VI – 170-2/4	8 19 95 –	15. Juli 1997

Der Bundesbeauftragte für den Datenschutz, Postf. 20 01 12, 53131 Bonn

An die
obersten Bundesbehörden

lt. Verteiler

Betr.: **Bearbeitung dienstlicher Vorgänge zu Hause auf privatem APC**

Anlg.: Merkblatt „Empfehlungen für die häusliche Verarbeitung dienstlicher Vorgänge auf privatem APC“

Es kann notwendig sein, dienstliche Vorgänge auch zu Hause unter Einsatz des häuslichen *privaten* APC bearbeiten zu können. Dies birgt für die Sicherheit der personenbezogenen Daten grundsätzlich die gleichen Risiken wie die Benutzung transportabler *dienstlicher* APC; ich habe hierauf in meinem 15. TB hingewiesen (Nr. 30.2). Die größte Gefahr – neben Verlieren, „Liegenlassen“, Diebstahl, Einbruch und Werkstattreparaturen – besteht in der Kenntnisnahme der gespeicherten Daten durch Unbefugte. Auch ist nicht allen Benutzern bekannt, daß gängige Textverarbeitungsprogramme unbemerkt automatisch Sicherheitskopien der auf Diskette mitgebrachten dienstlichen Daten auf dem privaten APC speichern. Zudem ist ein unwiderrufliches Löschen von Daten mit den standardmäßigen Löschbefehlen nicht möglich. Die Gefahr, daß auf der Festplatte des privaten Gerätes Kopien der dienstlichen Daten zurückbleiben, ist daher durchaus gegeben.

In der dienstlichen Arbeitsumgebung werden Risiken – entsprechend den Forderungen sowohl des Datenschutzes als auch der IT-Sicherheit – durch eine Risikoanalyse ermittelt und durch geeignete technische und organisatorische Maßnahmen eingegrenzt. Die auf diese Weise erreichte, gesetzlich geforderte Sicherheit darf beim häuslichen PC-Einsatz für die Verarbeitung dienstlicher Daten nicht „ersatzlos gestrichen werden“, vielmehr muß auch hier eine angemessene Sicherheit gewährleistet sein.

Anzustreben ist dabei in jedem Fall der Einsatz **dienstlicher** Notebooks usw., die über die dienstlichen Sicherheitskomponeten verfügen und ausschließlich für die Verarbeitung dienstlicher Daten genutzt werden dürfen, insbesondere in den Arbeitsgebieten, in denen besonders sensible Daten verarbeitet werden. Diese Geräte sollten dann dem jeweiligen Bearbeiter für die Dauer der Bearbeitung von der Dienststelle ausgeliehen werden.

Anhaltspunkte dafür, welche Daten als besonders sensibel anzusehen sind, enthält § 28 Abs. 2 Satz 2 BDSG, der für die Datenverarbeitung im Rahmen der Zweckbestimmung eines Vertragsverhältnisses oder vertragsähnlichen Vertrauensverhältnisses einen besonderen Schutz für Daten vorsieht, die sich z.B.

- auf gesundheitliche oder soziale Verhältnisse,
- auf strafbare Handlungen oder Ordnungswidrigkeiten,
- auf religiöse oder politische Anschauungen sowie
- auf dienst- oder arbeitsrechtliche Rechtsverhältnisse

beziehen.

Soweit und solange der Einsatz dienstlicher Notebooks u.ä. nicht möglich ist, empfehle ich die Beachtung der praxisbezogenen Regeln, die ich in dem als Anlage beigefügten Merkblatt zusammengestellt habe. Ich wäre Ihnen dankbar, wenn Sie das Merkblatt auch im nachgeordneten Bereich bekanntmachen würden.

Im Auftrag

Empfehlungen für die häusliche Bearbeitung dienstlicher Vorgänge auf privatem APC

Bei der häuslichen Bearbeitung dienstlicher Vorgänge auf privaten APC'n bestehen für die Sicherheit der personenbezogenen Daten grundsätzlich die gleichen Risiken wie in der dienstlichen Umgebung, jedoch zum Teil mit wesentlich erhöhter Eintretenswahrscheinlichkeit. Hierzu gehören Verlieren, „Liegenlassen", Diebstahl, Einbruch und Werkstattreparatur des APC. Besonders hoch ist das Risiko unbefugter Kenntnisnahme der Daten, denn grundsätzlich ist zu Hause jeder andere – Familienangehöriger, Besucher – Unbefugter.

Zur Begrenzung der Sicherheitsrisiken auf ein tragbares Maß sollten daher die folgenden

I. Grundsätze

beachtet werden:

(1) Die Verarbeitung dienstlicher Daten auf privaten APC sollte in einer Dienstanweisung bzw. Dienstvereinbarung geregelt sein.

(2) Der Fachvorgesetzte muß über Art und Umfang der Tätigkeit informiert werden und ihr zugestimmt haben. Bei zeitlich unbefristeter Tätigkeit sollte die Zustimmung schriftlich erfolgen.

(3) Art und Menge der nach Hause mitgenommenen Daten sind entsprechend den häuslichen Sicherungsmöglichkeiten und der jeweils möglichen Arbeitsleistung zu beschränken; keine Mitnahme ganzer Datenbanken (z.B. Personalinformationssystem der Dienststelle).

(4) Über Verlust, Diebstahl, Beschlagnahme usw. ist die Dienststelle unverzüglich zu informieren.

II. Technisch-organisatorische Maßnahmen

(1) Unterrichtung des behördlichen Datenschutzbeauftragten über Art und Umfang der häuslichen Verarbeitung.

(2) Installation von Sicherheitskomponenten auf dem APC durch die Dienststelle.

(3) Zur häuslichen Verarbeitung vorgesehene Daten werden nur in dem erforderlichen Umfang und von einem besonders benannten Mitarbeiter der Dienststelle auf Datenträger kopiert und nach Bearbeitung wieder ins dienstliche System eingestellt.

(4) Kryptographische Verschlüsselung aller Daten auf dem APC und den Datenträgern – auch auf Sicherungskopien – und bei Übertragung per E-Mail usw. zwischen Dienststelle und Wohnung.

(5) Sichere Aufbewahrung von dienstlichen Datenträgern sowie Paßwörtern und Kryptoschlüsseln.

(6) Während der Verarbeitung dienstlicher Daten den APC von allen Außenverbindungen physikalisch trennen (Leitungsstecker zum öffentlichen Telefonnetz ziehen).

(7) In angemessenen Zeitabständen Suche nach schädlichen Programmen (mittels „Virenscanner" usw.).

(8) Nicht (mehr) benötigte Ausdrucke ordnungsgemäß vernichten, ggf. in der Dienststelle.

(9) Nach Ende der Verarbeitung physikalische Löschung aller dienstlichen Daten.

(10) Vor externen Reparaturen am APC physikalische Löschung aller dienstlichen Daten. Ist dies nicht möglich, Übergabe der defekten Speicherbaugruppe an die Reparaturfirma nur mit Zustimmung der Dienststelle.

Anlage 21 (zu Nr. 10.1.9)

Der Bundesbeauftragte für den Datenschutz

Geschäftszeichen (bei Antwort bitte angeben) VI – 191/7 ☎ (02 28) 8 19 95 – Datum 3. Juli 1997

Der Bundesbeauftragte für den Datenschutz, Postf. 20 01 12, 53131 Bonn

An die
obersten Bundesbehörden

lt. Verteiler

Betr.: **Datenschutz beim Betrieb von Telekommunikationsanlagen (TK-Anlagen)**

Durch das am 1. August 1996 in Kraft getretene Telekommunikationsgesetz (TKG) wird der Geltungsbereich datenschutzrechtlicher Vorschriften erweitert, nämlich auf alle „Unternehmen, die geschäftsmäßig Telekommunikationsdienste erbringen oder an der Erbringung solcher Dienste mitwirken“. Hierzu gehören nach der amtlichen Begründung des Gesetzentwurfes zum § 85 Abs. 2 TKG auch Betreiber von „. . . Corporate Networks und Nebenstellenanlagen *(TK-Anlagen*) . . . in Betrieben und Behörden, soweit sie den Beschäftigten zur privaten Nutzung zur Verfügung gestellt sind“.

Neben den Vorschriften des TKG über das Fernmeldegeheimnis und den Datenschutz ist für die Betreiber von TK-Anlagen insbesondere die Telekommunikationsdienstunternehmen-Datenschutzverordnung (TDSV) von Bedeutung; auch diese Vorschriften sind vom o.g. Adressatenkreis zu beachten.

Die rechtlichen Verpflichtungen betreffen u.a. die Wahrung des Fernmeldegeheimnisses (§ 85 TKG), die Erhebung und Verarbeitung von Verbindungsdaten zur Entgeltermittlung und -abrechnung (§ 6 TDSV) und die Anzeige der Rufnummer des Anrufers beim Angerufenen (§ 9 TDSV).

Hiermit rege ich eine entsprechende Bekanntmachung in Ihrem Zuständigkeitsbereich an.

Im Auftrag

Anlage 22 (zu Nr. 10.1.9)

Der Bundesbeauftragte für den Datenschutz

Geschäftszeichen (bei Antwort bitte angeben)
VI – 191/7

☎ (02 28)
8 19 95 –

Datum
3. Juli 1997

Der Bundesbeauftragte für den Datenschutz, Postf. 20 01 12, 53131 Bonn

An die
Spitzenverbände aus Industrie und Wirtschaft

lt. Verteiler

Betr.: **Datenschutz beim Betrieb von Telekommunikationsanlagen (TK-Anlagen)**

Sehr geehrte Damen und Herren,

am 1. August 1996 ist das Telekommunikationsgesetz (TKG) in Kraft getreten. Durch das TKG wird der Geltungsbereich datenschutzrechtlicher Vorschriften erweitert, nämlich auf alle „Unternehmen, die geschäftsmäßig Telekommunikationsdienste erbringen oder an der Erbringung solcher Dienste mitwirken“. Hierzu gehören nach der amtlichen Begründung des Gesetzentwurfes zum § 85 Abs. 2 TKG auch Betreiber von „. . . Corporate Networks, Nebenstellenanlagen in Hotels und Krankenhäusern, Clubtelefonen und Nebenstellenanlagen in Betrieben und Behörden, soweit sie den Beschäftigten zur privaten Nutzung zur Verfügung gestellt sind“. Nebenstellenanlagen – heute zumeist TK-Anlagen genannt – in Hotels und Krankenhäusern gehören auch dann dazu, wenn sie auch von den Gästen bzw. Patienten genutzt werden dürfen.

Neben den Vorschriften des TKG über das Fernmeldegeheimnis und den Datenschutz ist für die Betreiber von TK-Anlagen insbesondere die Telekommunikationsdienstunternehmen-Datenschutzverordnung (TDSV), eine Rechtsverordnung der Bundesregierung, von Bedeutung; auch diese Vorschriften sind vom o.g. Adressatenkreis zu beachten.

Die rechtlichen Verpflichtungen betreffen u.a. die Wahrung des Fernmeldegeheimnisses (§ 85 TKG), die Erhebung und Verarbeitung von Verbindungsdaten zur Entgeltermittlung und -abrechnung (§ 6 TDSV) und die Anzeige der Rufnummer des Anrufers beim Angerufenen (§ 9 TDSV).

Nach meiner Erkenntnis sind diese Verpflichtungen noch nicht allen Mitgliedern Ihres Verbandes bekannt. Ich wäre Ihnen daher dankbar, wenn Sie diese baldmöglichst in geeigneter Weise dementsprechend informieren würden.

Mit der datenschutzrechtlichen Beratung und Kontrolle der genannten Unternehmen hat der Gesetzgeber mich beauftragt, soweit keine Kontrollzuständigkeit anderer Institutionen – etwa der Landesbeauftragten für den Datenschutz, z.B. für Krankenhäuser der Länder und Gemeinden – besteht. Ich stehe Ihnen in diesem Zusammenhang daher gern für Beratungen zur Verfügung.

Mit freundlichen Grüßen

Im Auftrag

Anlage 23 (zu Nr. 11.9)

Thesenpapier zu INPOL – neu – Protokollierung

Nach Auffassung der AG INPOL-neu der Datenschutzbeauftragten des Bundes und der Länder schreibt § 11 Abs. 6 des BKAG nur den Mindestumfang von Protokollierungen im polizeilichen Informationssystem (INPOL) vor, schließt jedoch eine weitergehende Protokollierung nicht aus.

Die Protokolldaten unterliegen in vollem Umfang der datenschutzrechtlichen Kontrolle.

Es ist daher wünschenswert, daß sämtliche Abrufe personenbezogener Daten des polizeilichen Informationssystems INPOL-neu vollständig protokolliert werden.

Die Nutzung dieser Protokolldaten hat sich auf die in § 11 Abs. 6 Satz 2 BKAG genannten Zwecke – die datenschutzrechtliche Kontrolle und die Sicherstellung eines ordnungsgemäßen Betriebes der Datenverarbeitungsanlage – zu beschränken. Die im Gesetz vorgesehene Zweckänderung der Nutzung der Protokolldaten für kriminalpolizeiliche Belange birgt Gefahren in sich, denen durch flankierende Maßnahmen entgegenzutreten ist. Solche Maßnahmen sind besondere Aufzeichnungspflichten und Genehmigungsvorbehalte für eine zweckdurchbrechende Nutzung sowie eine zeitnahe Unterrichtung des Bundesbeauftragten für den Datenschutz.

Darüber hinaus ist vom System automatisiert, also unabhängig von der Einzelfallentscheidung, jede Verwendung der Protokolldaten aufzuzeichnen.

Anlage 24 (zu Nr. 11.9)

Positionspapier 1 der AG INPOL-neu der Datenschutzbeauftragten zum Kriminalaktennachweis

Die Arbeitsgruppe INPOL-neu der Datenschutzbeauftragten des Bundes und der Länder hat gegenüber der Projektgruppe INPOL-neu beim BKA mit Schreiben des Bundesbeauftragten für den Datenschutz vom 23. Oktober 1998, V – 642 – 1/13, zum Informationsumfang des KAN im Rahmen von INPOL-neu darauf hingewiesen, daß § 2 Abs. 1 des BKAG **abschließend** den Datenumfang festlegt. Somit sind nur „Straftaten von länderübergreifender, internationaler oder erheblicher Bedeutung“ INPOL-relevant. Der eindeutige Gesetzestext läßt keinen Platz für weitergehende Auslegungen.

Die Projektgruppe „Fachfragen“ gibt in ihrem Abschlußbericht vom 24. November 1998 zu erkennen, daß unter Hinweis auf die Begründung zu § 2 Abs. 2 des BKAG weitere personenbezogene Speicherungen im KAN möglich sein sollen, *„wenn aufgrund der Umstände des Einzelfalls eine kriminalistische Prognose des jeweiligen Sachbearbeiters zu dem Schluß führt, durch die Bereitstellung der Informationen in den Verbund kann zur Verhütung oder Verfolgung entsprechender Straftaten beigetragen werden“.*

Aus dem Gesetzgebungsverfahren ist bekannt, daß dies bei Überlegungen zu INPOL und auch zu EUROPOL eine Rolle gespielt hat. Sie sind jedoch durch den vom Gesetzgeber beschlossenen Text bezüglich des polizeilichen Informationssystems INPOL (KAN) nicht übernommen worden. Ein Rückgriff auf die Gesetzesbegründung verbietet sich daher.

Deshalb weist die Arbeitsgruppe INPOL-neu der Datenschutzbeauftragten darauf hin, daß nur solche Informationen in INPOL-neu zur Verfügung gestellt werden dürfen, die bereits zum Übermittlungszeitpunkt im Einzelfall die Kriterien des § 2 Abs. 1 BKAG erfüllen. Die Kriterien werden im Abschlußbericht der Projektgruppe Fachfragen viel zu weit ausgelegt. Eine fachliche Erforderlichkeit für eine solche Auslegung ist nicht nachzuvollziehen. Sie übertrifft sogar die bereits sehr weit gefaßten Formulierungen der Rahmenrichtlinien zum Kriminalaktennachweis von 1990, die dringend der bestehenden Gesetzeslage angepaßt werden müssen.

Anlage 25 (zu Nr. 11.9)

Positionspapier 2 der AG INPOL-neu der Datenschutzbeauftragten zum Kriminalaktennachweis

Auch für den Informationsumfang des Kriminalaktennachweises (KAN) im Rahmen von INPOL-neu ist nach Auffassung der AG INPOL-neu der Datenschutzbeauftragten die in § 2 Abs. 1 BKAG einfachgesetzlich definierte Reichweite der Zentralstellenfunktion des BKA gem. Artikel 87 Abs. 1 Satz 2 GG maßgeblich. Dies bedeutet, daß auch weiterhin lediglich „Straftaten mit länderübergreifender, internationaler oder erheblicher Bedeutung“ INPOL-relevant sein können. § 2 Abs. 3 BKAG hebt den Betrieb von INPOL als Konkretisierung der Zentralstellenfunktion gemäß dessen Abs. 1 hervor (vgl. die Gesetzesbegründung zu § 2 Abs. 2 und 3), ohne insoweit von der dort festgelegten Relevanzschwelle abzuweichen. Demgegenüber fehlt ein entsprechender qualifizierender Zusatz etwa in § 2 Abs. 4 BKAG für erkennungsdienstliche Sammlungen. Desweiteren wird auch in § 8 Abs. 1 BKAG, der für BKA und Länderpolizeien eine rechtliche Obergrenze für die Übermittlung von Daten an INPOL darstellt, u.a. auf § 2 Abs. 1 BKAG verwiesen.

Überlegungen der Projektgruppe INPOL-neu des BKA, wonach unter bestimmten Voraussetzungen zu einer Person auch nicht INPOL-relevante Fälle im Rahmen der „Fallkurzauskunft“ des künftigen KAN zur Verfügung gestellt werden sollen, um deren kriminelle Historie umfassender abzubilden, gehen daher über diese Rechtsgrundlage hinaus. Das BKAG verlangt die Bewertung jeder in INPOL einzustellenden Straftat nach den Kriterien der überörtlichen oder erheblichen Bedeutung. Dies setzt einem stärker personenorientierten Bewertungsansatz, der INPOL-neu offenbar zugrunde gelegt werden soll, rechtliche Grenzen.

Sowohl eine Verfahrensweise, nach der bei der ersten INPOL-relevanten Tat einer Person über Referenzen auch deren übrige Taten unterhalb der Relevanzschwelle des § 2 Abs. 1 BKAG abfragbar würden („Vorschlag A“), als auch eine sofortige Einstellung nicht INPOL-relevanter Fälle in den Verbund mit der Folge, daß diese bis zum ersten relevanten Fall einem eingeschränkten Nutzerkreis zur Verfügung gestellt würden („Vorschlag B“), wäre daher datenschutzrechtlich nicht tragbar.

Anlage 26 (zu Nr. 18.2.2)

Bitte	– füllen Sie den Personalbogen handschriftlich (gut leserlich z. B. in Blockschrift) oder aber mit der Schreibmaschine aus – beantworten Sie die Fragen sehr sorgfältig und vollständig

Lichtbild (Bitte ein Paßbild neuen Datums beifügen. Schreiben Sie bitte auf die Rückseite des Paßbildes: Jahr der Aufnahme, Ihren Namen und Ihre Anschrift).
Jahr der Aufnahme

Personalbogen I

(Vorauswahl)

1. Angaben zu meiner Person

Name (ggf. akadem. Grad)		
Vorname (bitte sämtliche Vornamen angeben, Rufnamen unterstreichen)		
Geburtsname/früherer Name		
Geburtsdatum	Geburtsort/Kreis/Bundesland	
Anschrift		
Telefon privat	Telefon dienstlich	

Staatsangehörigkeit		
☐ deutsch	☐ EU	☐ andere

Schwerbehindert		Einem Schwerbehinderten gleichgestellt	
☐ nein	☐ ja	☐ nein	☐ ja

2. Angaben über Schulausbildung, Hoch- und Fachschulstudium (einschl. Verwaltungsakademie)

Schulart, Studienrichtung	Dauer von – bis	Abschluß bzw. Abgang aus Klasse (ggf. voraussichtl. Abschluß, Abgang)

3. Angaben über abgelegte Prüfungen
(z. B. Abschlußprüfung in einem Ausbildungsberuf, Studienabschluß, Laufbahnprüfung)

Bezeichnung der Prüfung	Datum	Note

Promotion zum, am	Ergebnis
Dissertationsthema:	

4. Angaben über besondere Kenntnisse

Sprachkenntnisse/Sprache	Ausbildungs-stand*)	
Englisch		*) Den Ausbildungsstand bitte wie folgt in Ziffern angeben: 1 Grundkenntnisse 2 Umgangssprache 3 fließend in Wort und Schrift 4 verhandlungssicher
Französisch		
Führerscheine ☐ ja ☐ nein	Falls ja: Welche Fahrerlaubnisklassen:	

Kurzschrift (nur bei Bewerbungen für den Schreibdienst)

nein ja	Silbenzahl

Maschinenschrift (nur bei Bewerbungen für den Schreibdienst)

nein ja	Anschläge/min

Sonstige besondere Kenntnisse

5. Wehr- oder Zivildienst

☐ ja	☐ nein

Dauer und Angabe der hierbei erworbenen besonderen Kenntnisse

6. Angaben über berufl. Tätigkeit
(einschl. Berufsausbildung, Praktikantenzeit, Zeiten der Nichtbeschäftigung)

Zeitraum (von – bis; lückenlose Angaben in zeitlicher Reihenfolge)	Arbeitgeber/Dienststelle, Ort, Art der Tätigkeit und Arbeitsgebiet

7. Angaben über den Bezug einer Altersrente oder Versorgungsbezüge als Ruhestandsbeamter

Erhalten Sie eine Altersrente aus der gesetzlichen Rentenversicherung oder Versorgungsbezüge als Ruhestandsbeamter?
☐ ja ☐ nein

8. Bei <u>Beamten</u> Angabe der <u>letzten</u> Ernennung

Amtsbezeichnung/Besoldungsgruppe	Jahr der Ernennung

Ich versichere, daß die vorstehenden Angaben vollständig sind und der Wahrheit entsprechen. Mir ist bekannt, daß falsche oder unvollständige Angaben ein evtl. Beschäftigungsverhältnis gefährden können.

Ort, Datum, Unterschrift

Erklärung zum Personalbogen I und II (nur für Beamte)

Erklärung über die Treuepflicht zum Grundgesetz

1. Belehrung

Nach § 7 Abs. 1 Nr. 2 des Bundesbeamtengesetzes ist der Beamte verpflichtet, sich durch sein gesamtes Verhalten zu der freiheitlichen demokratischen Grundordnung im Sinne des Grundgesetzes zu bekennen und für deren Erhalt einzutreten. Dementsprechend darf als Beamter nur eingestellt werden, wer die Gewähr bietet, daß er jederzeit für die freiheitliche demokratische Grundordnung im Sinne des Grundgesetzes eintritt.

Freiheitlich demokratische Grundordnung im Sinne des Grundgesetzes ist nach der Rechtsprechung des Bundesverfassungsgerichtes (vgl. Urt. vom 23. Oktober 1952 – 1 BvB/51 – BVerfGE 2, 1; Urt. vom 17. August 1956 – 1 BvB/51 – BVerfGE 5, 85) eine Ordnung, die unter Ausschluß jeglicher Gewalt- und Willkürherrschaft eine rechtsstaatliche Herrschaftsordnung auf der Grundlage der Selbstbestimmung des Volkes nach dem Willen der jeweiligen Mehrheiten und der Freiheit und Gleichheit darstellt. Die freiheitliche demokratische Grundordnung ist das Gegenteil des totalitären Staates, der als ausschließliche Herrschaftsmacht Menschenwürde, Freiheit und Gleichheit ablehnt. Zu den grundlegenden Prinzipien der freiheitlichen demokratischen Grundordnung sind insbesondere zu rechnen:

- Die Achtung vor den im Grundgesetz konkretisierten Menschenrechten, vor allem vor dem Recht auf Leben und freie Entfaltung der Persönlichkeit,
- Volkssouveränität,
- die Gewaltenteilung,
- die Verantwortlichkeit der Regierung gegenüber der Volksvertretung,
- die Gesetzmäßigkeit der Verwaltung,
- die Unabhängigkeit der Gerichte,
- das Mehrparteienprinzip,
- die Chancengleichheit für alle politischen Parteien,
- das Recht auf verfassungsmäßige Bildung und Ausübung der Opposition.

Die Teilnahme an Bestrebungen, die sich gegen diese Grundsätze richten, ist unvereinbar mit den Pflichten eines Beamten. Beamte, die sich einer solchen Pflichtverletzung schuldig machen, müssen mit ihrer Entlassung rechnen.

2. Erklärung

Ich bin über meine Pflicht zur Verfassungstreue und darüber belehrt worden, daß meine Teilnahme an Bestrebungen, die gegen die freiheitliche demokratische Grundordnung oder gegen ihre grundlegenden Prinzipien gerichtet sind, mit den Pflichten eines Beamten unvereinbar sind. Aufgrund der mir erteilten Belehrung erkläre ich hiermit, daß ich meine Pflicht zur Verfassungstreue stets erfüllen werde, daß ich die Grundsätze der freiheitlichen demokratischen Grundordnung im Sinne des Grundgesetzes bejahe und daß ich bereit bin, mich jederzeit durch mein gesamtes Verhalten zu der freiheitlichen demokratischen Grundordnung im Sinne des Grundgesetzes zu bekennen und für deren Erhaltung einzutreten.

Ich versichere ausdrücklich, daß ich in keiner Weise Bestrebungen unterstütze, deren Ziele gegen die freiheitliche demokratische Grundordnung oder gegen eines ihrer grundlegenden Prinzipien gerichtet sind.

Ich bin mir bewußt, daß beim Verschweigen einer solchen Unterstützung die Ernennung zum Beamten als durch arglistige Täuschung herbeigeführt angesehen wird. Arglistige Täuschung führt zur Entlassung (vgl. § 12 Abs. 1 Nr. 1 Bundesbeamtengesetz).

Ort, Datum

____

Unterschrift

____

Bitte	– füllen Sie den Personalbogen handschriftlich (gut leserlich z. B. in Blockschrift) oder aber mit der Schreibmaschine aus – beantworten Sie die Fragen sehr sorgfältig und vollständig

Personalbogen II

(ergänzende Fragen an grundsätzlich geeignete Bewerber)

1. Angaben zu meiner Person

Name (ggf. akadem. Grad), Vorname (bitte sämtliche Vornamen angeben, Rufnamen unterstreichen) (im übrigen wird auf Personalbogen I verwiesen)		
Bei Schwerbehinderung	Grad der Behinderung	Art der Behinderung (Beantwortung freigestellt)

Anerkannt/Festgestellt/Einem Schwerbehinderten gleichgestellt durch (Behörde, Datum, Aktenzeichen)

2. Angaben zu meinen Eltern/meinen gesetzlichen Vertretern

(nur bei minderjährigen Bewerbern)

Vater (Name, Vorname)
Geburtsname
Mutter (Name, Vorname)
Geburtsname

3. Angaben über Strafen und Disziplinarmaßnahmen

Strafen[1]) und Disziplinarmaßnahmen (soweit nicht getilgt) und laufende Verfahren. – Datum, Höhe, Grund der Bestrafung/Disziplinamaßnahme – Art und Grund eines laufenden Verfahrens – Gericht/Behörde und Aktenzeichen

1) Gemäß § 53 Abs. 1 des Gesetzes über das Zentralregister und das Erziehungsregister – BZRG – vom 21. September 1994 braucht der Verurteilte Verurteilungen und den der Verurteilung zugrundliegenden Sachverhalt nicht zu offenbaren, wenn die Verurteilungen nicht in ein Führungszeugnis aufzunehmen oder getilgt sind.

4. Angaben über wirtschaftliche Verhältnisse

1. Haben Sie die Eidesstattliche Versicherung abgegeben?

☐ ja ☐ nein

2. Laufen gegen Sie zur Zeit Pfändungs- oder Überweisungsbeschlüsse?

☐ ja ☐ nein

5. Ehrungen und Auszeichnungen

6. Änderungen zu den Angaben im Personalbogen I

☐ Es haben sich zwischenzeitlich keine Änderungen ergeben

☐ Es haben sich folgende Veränderungen ergeben (bitte im einzelnen angeben, was sich geändert hat, ggf. auf gesondertem Blatt)

Ich versichere die Richtigkeit und Vollständigkeit der vorstehenden Angaben. Die möglichen Folgen unrichtiger Angaben – Auflösung des bestehenden Arbeitsverhältnisses – sind mir bekannt.

____________________________ ____________________________

(Ort, Datum) (Unterschrift)

Anlage 1 zum Personalbogen II

(Nur von Bewerbern auszufüllen, die ihren Wohnsitz bis zum 9. November 1989 im Beitrittsgebiet hatten *)

1. Haben Sie vor dem 9. November 1989 ein Amt oder eine Funktion in der SED, in Massenorganisationen/ gesellschaftlichen Organisationen oder eine sonstige herausgehobene Funktion im System der DDR innegehabt?

Wenn ja, bitte nachstehend erläutern:

☐ ja ☐ nein

SED/Organisation	Amt/Funktion	von/bis

2. Waren Sie Mitarbeiter des Ministeriums für Staatssicherheit oder beim Amt für nationale Sicherheit?

Wenn ja, welcher Art war diese Tätigkeit (auch inoffiziell) und von welcher Dauer (von/bis) war sie?

☐ ja ☐ nein

(Dauer/Art der Tätigkeit; evtl. kurze Begründung)

3. Angaben über Dienstlaufbahn (Ernennungen, Beförderungen usw.)

	Dienstgrad/Dienstbezeichnung	ab (Datum)

*) Anfragen (Auskunftsersuchen) an den Bundesbeauftragten für die Unterlagen des Staatssicherheitsdienstes der ehemaligen DDR erfolgen in den im Erlaß des Bundesministeriums des Innern vom 5. September 1994 und in hierzu ggf. ergangenen Änderungserlassen genannten Fällen. Bei diesen Anfragen ist zu unterscheiden zwischen

1. den Anfragen, die aus Anlaß von Personalmaßnahmen (Einstellung in den oder Beschäftigung/Weiterverwendung im öffentlichen Dienst des Bundes) durch die für die Personal- und Stellenbewirtschaftung zuständigen Stellen (s. §§ 20, 21 Abs. 1 Nr. 6 Buchst. d und Nr. 7 Buchst. f StUG) erfolgen, und
2. den Anfragen, die im Rahmen von Sicherheitsüberprüfungen nach § 12 Abs. 4 SÜG vom 20. April 1994 (BGBl. I S. 867) durchgeführt werden (vgl. hierzu auch VwV des Bundesministeriums des Innern vom 29. April 1994 GMBl. S. 550 i.d.F. der mit Rundschreiben des Bundesministeriums des Innern vom 6. Juni und 24. November 1997 bekanntgegebenen Änderungen).

Auskünfte des Bundesbeauftragten für die Unterlagen des Staatssicherheitsdienstes der ehemaligen DDR nach Nr. 1 werden zu der Personalakte in einem verschlossenen Umschlag, zu Nr. 2 zu der Sicherheitsakte des Betroffenen genommen.

Ich versichere die Richtigkeit und Vollständigkeit der vorstehenden Angaben. Die möglichen Folgen unrichtiger Angaben – Auflösung des bestehenden Arbeitsverhältnisses – sind mir bekannt.

______________________________ ______________________________

(Ort, Datum) (Unterschrift)

Erklärung zu Anlage 1 des Personalbogens II

Erklärung über die Treuepflicht zum Grundgesetz und Unterrichtung über außerordentliche Kündigungsmöglichkeiten nach Anlage I, Kap. XIX, Sachgebiet A, Abschnitt III, Nr. 1, Absatz 5 des Einigungsvertrages

1. Belehrung

Jeder Beschäftigte ist verpflichtet, sich durch sein gesamtes Verhalten zu der freiheitlichen demokratischen Grundordnung im Sinne des Grundgesetzes zu bekennen.

Freiheitliche demokratische Grundordnung im Sinne des Grundgesetzes ist nach der Rechtsprechung des Bundesverfassungsgerichtes (vgl. Urt. vom 23. Oktober 1952 – 1 BvB/51 – BVerfGE 2, 1; Urt. vom 17. August 1956 – 1 BvB/51 – BVerfGE 5, 85) eine Ordnung, die unter Ausschluß jeglicher Gewalt- und Willkürherrschaft eine rechtsstaatliche Herrschaftsordnung auf der Grundlage der Selbstbestimmung des Volkes nach dem Willen der jeweiligen Mehrheiten und der Freiheit und Gleichheit darstellt. Die freiheitliche demokratische Grundordnung ist das Gegenteil des totalitären Staates, der als ausschließliche Herrschaftsmacht Menschenwürde, Freiheit und Gleichheit ablehnt. Zu den grundlegenden Prinzipien der freiheitlichen demokratischen Grundordnung sind insbesondere zu rechnen:

- Die Achtung vor den im Grundgesetz konkretisierten Menschenrechten, vor allem vor dem Recht auf Leben und freie Entfaltung der Persönlichkeit,
- Volkssouveränität,
- die Gewaltenteilung,
- die Verantwortlichkeit der Regierung gegenüber der Volksvertretung,
- die Gesetzmäßigkeit der Verwaltung,
- die Unabhängigkeit der Gerichte,
- das Mehrparteienprinzip,
- die Chancengleichheit für alle politischen Parteien,
- das Recht auf verfassungsmäßige Bildung und Ausübung der Opposition.

Die Teilnahme an Bestrebungen, die sich gegen diese Grundsätze richten, ist unvereinbar mit den Pflichten eines Beschäftigten.

Beschäftigte, die sich einer solchen Pflichtverletzung schuldig machen, müssen mit ihrer Entlassung rechnen.

2. Erklärung

Ich bin über meine Pflicht zur Verfassungstreue und darüber belehrt worden, daß meine Teilnahme an Bestrebungen, die gegen die freiheitliche demokratische Grundordnung oder gegen ihre grundlegenden Prinzipien gerichtet sind, mit den Pflichten eines Beschäftigten unvereinbar sind. Aufgrund der mir erteilten Belehrung erkläre ich hiermit, daß ich meine Pflicht zur Verfassungstreue stets erfüllen werde, daß ich die Grundsätze der freiheitlichen demokratischen Grundordnung im Sinne des Grundgesetzes bejahe und, daß ich bereit bin, mich jederzeit durch mein gesamtes Verhalten zu der freiheitlichen demokratischen Grundordnung im Sinne des Grundgesetzes zu bekennen.

Ich versichere ausdrücklich, daß ich in keiner Weise Bestrebungen unterstütze, deren Ziele gegen die freiheitliche demokratische Grundordnung oder gegen eines ihrer grundlegenden Prinzipien gerichtet sind.

Ich bin mir bewußt, daß beim Verschweigen einer solchen Unterstützung das Arbeitsverhältnis aufgelöst werden kann.

Mir ist bekannt, daß gemäß Anlage I, Kap. XIX, Sachgebiet A, Abschnitt III, Nr. 1 Absatz 5 zum Einigungsvertrag ein wichtiger Grund für eine außerordentliche Kündigung insbesondere dann gegeben ist, wenn der Arbeitnehmer

1. gegen die Grundsätze der Menschlichkeit oder Rechtsstaatlichkeit verstoßen hat, insbesondere die im Internationalen Pakt über bürgerliche und politische Rechte vom 19. Dezember 1966 gewährleisteten Menschenrechte oder die in der Allgemeinen Erklärung der Menschenrechte vom 10. Dezember 1948 enthaltenen Grundsätze verletzt hat oder
2. für das frühere Ministerium für Staatssicherheit/Amt für nationale Sicherheit tätig war

und deshalb ein Festhalten am Arbeitsverhältnis unzumutbar erscheint.

Ort, Datum ______________________________

Unterschrift ______________________________

Anlage 27 (zu Nr. 8.5)

Arbeitspapier „Datenschutzfreundliche Technologien“

herausgegeben vom Arbeitskreis „Technische und organisatorische Datenschutzfragen“
der Konferenz der Datenschutzbeauftragten des Bundes und der Länder

Stand: 1. Oktober 1997

1. Einleitung

Die Computertechnologie ist in alle Lebensbereiche eingedrungen und breitet sich mehr und mehr aus. Beim Einkaufen, Zahlen, Buchen und Reservieren mittels bequemer Chip- oder Magnetstreifenkarten, bei der Kommunikation mittels digitaler Netze, bei Arztbesuchen mit Krankenversichertenkarten oder evtl. zukünftig mit Patientenkarten, auch durch Teilnahme an Online-Diensten sowie an nationalen und internationalen Netzwerken fallen eine Fülle von Einzeldaten über den Nutzer an. Diese elektronischen Spuren sind geeignet, persönliche Profile über den Einzelnen hinsichtlich seines Verhaltens zu bilden.

Immer mehr Bürger benutzen diese Technologie. Doch nicht zuletzt aufgrund der Komplexität und der mangelnden Transparenz von Systemen der modernen Informations- und Kommunikationstechnik (IuK-Technik) für die Nutzer, fehlen diesen in der Regel Kenntnis und Kontrolle über Art, Umfang, Speicherort, Speicherdauer und Verwendungszweck der über sie erhobenen und gespeicherten Daten.

Der Schutz der Privatheit des Einzelnen wird bei Nutzung dieser Systeme bisher vorwiegend dadurch angestrebt, daß der Zugang zu den erhobenen, gespeicherten und verarbeiteten personenbezogenen Daten mittels technischer und organisatorischer Maßnahmen beschränkt wird. Der Schutz der Privatheit des Einzelnen hängt somit lediglich von der Wirksamkeit der üblichen Sicherheitsmaßnahmen und der Gewissenhaftigkeit ab, mit der sie durchgeführt werden. Mit diesen Sicherheitsmaßnahmen werden nur die klassischen Schutzziele Integrität, Vertraulichkeit, Verfügbarkeit und Zurechenbarkeit der gespeicherten Daten verfolgt.

Es wächst die Erkenntnis, daß der zunehmenden Gefährdung der Privatheit des Einzelnen nur durch eine weitgehende Reduzierung der Menge der gespeicherten Daten wirksam begegnet werden kann. Die Nutzung von IuK-Technik durch natürliche Personen wird demzufolge auch zukünftig nur dann den Ansprüchen der Datenschutzfreundlichkeit gerecht, wenn sie nach dem Prinzip der **Datensparsamkeit** erfolgt, *wobei so wenig personenbezogene Daten wie möglich* erhoben, gespeichert

und verarbeitet werden. **Datenvermeidung** ist die stets anzustrebende Form der Datensparsamkeit. In diesem Fall werden bei der Nutzung von IuK-Systemen *keine personenbezogenen Daten* erhoben, gespeichert und verarbeitet, die Nutzung der IuK-Systeme erfolgt also anonym. Inhaltlich sind diese Forderungen Bestandteil des in den Datenschutzgesetzen des Bundes und der Länder festgelegten Grundsatzes der Erforderlichkeit, der auch schon bisher bei der Ausgestaltung der IuK-Technik zu beachten war, allerdings mit der technischen Entwicklung zunehmende Bedeutung gewinnt.

Anhand von Betrachtungen konkreter Beispiele aus dem Medienbereich, dem elektronischen Zahlungsverkehr, dem Gesundheitsbereich, der Telekommunikation sowie aus den Bereichen Transport und Verkehr werden in der Anlage die in diesen Projekten gewählten Ansätze und Bemühungen zur Verwendung datenschutzfreundlicher Technologien aufgezeigt. Es werden Empfehlungen in allgemeiner Form und für den jeweiligen Bereich gegeben.

2. Notwendigkeit für Datenschutz durch Technik

2.1 Rechtliche Forderungen und Entwicklungen

Bereits 1983 hat das Bundesverfassungsgericht im Volkszählungsurteil – am Beispiel der Statistik – den Anspruch auf Anonymisierung anerkannt. Gemäß der bekannten Auffassung des Bundesverfassungsgerichts heißt es dort: „Für den Schutz des Rechts auf informationelle Selbstbestimmung ist – und zwar auch schon für das Erhebungsverfahren – ... die Einhaltung des Gebots einer möglichst frühzeitigen faktischen Anonymisierung unverzichtbar, verbunden mit Vorkehrungen gegen die Deanonymisierung“ (BVerfGE 65, 1, 49). In der Rechtsprechung zum Medienrecht ist das Recht auf Anonymität ebenfalls seit längerem als besondere Ausprägung des Persönlichkeitsrechts anerkannt, beispielsweise vom Bundesgerichtshof: „Das Recht auf informationelle Selbstbestimmung schützt ... davor, aus dem Bereich der Anonymität in den einer persönlichen Bekanntheit gerückt zu werden“ (BGH AfP 1994, 306, 307).

Auch der Rat für Forschung, Technologie und Innovation, der unter Federführung des Bundeskanzleramts und des Bundesministers für Bildung, Wissenschaft, Forschung und Technologie einen ausführlichen Bericht über Chancen, Innovationen und Herausforderungen der Informationsgesellschaft erstellt hat, hat das Thema Anonymisierung aufgegriffen. Der Rat führt in Kap. 2.5 über Datenschutz folgendes aus: „Den Vorrang verdienen Verfahren, die den Betroffenen ein Höchstmaß an Anonymität gegenüber Netzbetreibern und Dienstleistungsanbietern sichern“. Entsprechende Passagen finden sich auch in den Bundestags- und Bundesratsdrucksachen über „Deutschlands Weg in die Informationsgesellschaft“ wieder [BD776].

Der Grundsatz der Datenvermeidung ist auch im Informations- und Kommunikationsdienste-Gesetz (IuKDG), dort in Artikel 2 Teledienstedatenschutzgesetz (TDDSG), und im Mediendienste-Staatsvertrag [MDStV] enthalten. Danach haben Anbieter von Tele- bzw. Mediendiensten den Nutzern die Inanspruchnahme und Bezahlung entweder vollständig anonym oder unter Verwendung eines Pseudonyms zu ermöglichen, soweit dies technisch möglich und zumutbar ist [IuKDG].

Die europäische Richtlinie zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten sowie zum freien Datenverkehr [95/46/EG] enthält den Grundsatz, daß eine Verarbeitung personenbezogener Daten nur stattfinden darf, soweit sie im Hinblick auf bestimmte und festgelegte Zwecke notwendig ist. Sie geht deshalb auch von dem Prinzip aus, daß das Recht auf Privatsphäre und Selbstbestimmung dadurch am wirksamsten geschützt wird, daß möglichst keine personenbezogenen Daten erhoben werden. Im Hinblick auf die Umsetzung dieses Grundsatzes fördert die Europäische Kommission die Entwicklung und Anwendung datenschutzfreundlicher Technologien, insbesondere im Rahmen des elektronischen Handels, sowie beispielsweise die Möglichkeit anonymen Zugangs zu Netzen und anonyme Zahlungsweisen.

2.2 Grundlegende Betrachtung von Informationssystemen

Betrachtet man traditionelle *informationsverarbeitende Systeme in ihrer komplexen Gesamtheit*, so sind einige klassische Einzelprozesse (Systemelemente) identifizierbar, in denen üblicherweise solche Daten, die zur Identifizierung des Benutzers geeignet sind, anfallen, bearbeitet und gespeichert werden:

1. **Autorisierung** (Vergabe einer Berechtigung und eines Berechtigungsprofils zur Nutzung des Systems z. B. bei Vertragsabschluß, Personalisierung von Chipkarten usw.)
2. **Identifikation und Authentikation** (Nachweisführung des Benutzers über seine grundsätzliche Berechtigung zur Nutzung des Systems)
3. **Zugriffskontrolle** (Prüfung des Berechtigungsprofils relativ zu der gewünschten Aktion/Dienstleistung des Systems)
4. **Protokollierung** (Festhalten von Aktionen gemeinsam mit Angaben zum Benutzer zum Zwecke der Nachweisführung)
5. **Abrechnung** (Rechnungsstellung der erbrachten und in Anspruch genommenen Systemleistungen an den Benutzer)

Als Begründung für die jeweils erhobenen, anfallenden, gespeicherten und verarbeiteten personenbezogenen Daten werden überwiegend Abrechnungszwecke, verbesserte Kundenbetreuung, statistische sowie Kontrollzwecke angegeben.

Die tatsächliche Identität des Benutzers ist für die Funktionalität eines IuK-Systems grundsätzlich jedoch nicht erforderlich. Allenfalls in bestimmten Fällen zur Autorisierung, Abrechnung und Protokollierung könnte die tatsächliche Identität des Benutzers erforderlich sein und müßte dort offengelegt werden bzw. bekannt sein. In den übrigen Prozessen ist dies nicht notwendig RGB95.

Wenn in einem System stattfindende Aktionen überwacht werden müssen und diese Überwachung nicht ausschließlich innerhalb des Systems möglich ist, so ist eine Protokollierung erforderlich. So ist z. B. die in den Datenschutzgesetzen des Bundes und der Länder vorgeschriebene Eingabekontrolle (z. B. Nr. 7 der Anlage zu § 9 BDSG) i.d.R. nur mit Hilfe der Protokollierung realisierbar, da die Zulässigkeit der Datenerhebung bzw. der Datenspeicherung nicht maschinell geprüft werden kann.

Bereits bei der Konzeption von IuK-Systemen sollte daher generell und für jeden einzelnen Prozeß untersucht werden, ob Daten zur wahren Identität des Einzelnen zur Verfügung stehen müssen oder ob eine anonyme oder pseudonyme Gestaltung in Frage kommt (siehe Abschnitte „Anonymisierung“ und „Pseudonymisierung“).

3. Anonymisierung

Anonymisierung ist eine Veränderung personenbezogener Daten derart, daß die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können.

In den Datenschutzgesetzen von Bund und Ländern ist Anonymisierung unterschiedlich definiert. So ist in einigen Datenschutzgesetzen (z. B. § 3 Abs. 7 BDSG, Artikel 4 Abs. 8 BayDSG, § 3 Abs. 7 LDSG RP, § 2 Abs. 7 DSG-LSA) für eine Anonymisierung bereits „das Verändern personenbezogener Daten derart, daß die Einzelangaben über persönliche oder sachliche Verhältnisse *nicht mehr oder nur mit einem unverhältnismäßig hohen Aufwand an Zeit, Kosten und Arbeitskraft* einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können“ ausreichend. Andere Datenschutzgesetze (z. B. § 3 Abs. 7 Nr. 5 DSG MV, § 3 Abs. 2 Nr. 4 SächsDSG, § 2 Abs. 2 Nr. 7 LDSG SH) stellen höhere Anforderungen. Hier wird unter Anonymisieren „das Verändern personenbezogener Daten derart, daß die Einzelangaben über persönliche oder sachliche Verhältnisse *nicht mehr* einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können“, verstanden.

Die Qualität der Anonymisierungsprozedur hängt von verschiedenen Einflußfaktoren ab. Entscheidend hierfür sind der Zeitpunkt der Anonymisierung, die Rücknahmefestigkeit der Anonymisierungsprozedur, die Mächtigkeit der Menge, in der sich der Betroffene verbirgt, und die Verkettungsmöglichkeit von einzelnen Transaktionen desselben Betroffenen.

Auch konkrete Einzelangaben in einem Datensatz/einer Transaktion (z. B. Beruf/Amt=Bundeskanzler, konkrete Einkommensangaben) sind für die Qualität der Anonymisierungsprozedur von Bedeutung und können die Mächtigkeit der Menge, in der sich der Betroffene verbirgt, verringern. Sind im Wertebereich Werte vorhanden, die die Anonymität gefährden, müssen sie mit anderen zusammengefaßt werden. Ist eine solche Veränderung aus technischen oder inhaltlichen Gründen nicht möglich, kann keine Anonymität erreicht werden.

Das Ziel datenschutzfreundlicher Technologien ist es unter anderem, Daten schon ohne Personenbezug zu erheben oder bereits personenbezogen erhobene Daten so bald wie möglich zu anonymisieren. Ein Höchstmaß an Anonymität wird erreicht, wenn personenbezogene Daten gar nicht erst entstehen. Gelungene Beispiele hierfür sind anonyme Telefonkarten und anonyme Zahlkarten im öffentlichen Personennahverkehr. Beispiele für die Anwendung der Anonymisierung sind im Bereich der Statistik und in der Forschung zu finden.

4. Pseudonymisierung

Pseudonymisierung ist das Verändern personenbezogener Daten durch eine Zuordnungsvorschrift derart, daß die Einzelangaben über persönliche oder sachliche Verhältnisse ohne Kenntnis oder Nutzung der Zuordnungsvorschrift nicht mehr einer natürlichen Person zugeordnet werden können.

Dazu werden beispielsweise die Identifikationsdaten durch eine Abbildungsvorschrift in ein willkürlich gewähltes Kennzeichen (das Pseudonym) überführt. Ziel eines solchen Verfahrens ist es, nur bei Bedarf und unter Einhaltung vorher definierter Rahmenbedingungen den Personenbezug wieder herstellen zu können. Die Reidentifizierung kann mitunter auch ausschließlich dem Betroffenen vorbehalten bleiben. Mit Referenz- und Einweg-Pseudonymen (siehe folgende Unterabschnitte) versehene Daten sind jedoch weiterhin personenbezogene Daten, da sie einer bestimmten oder bestimmbaren Person zugeordnet werden können.

Das Mittel der Pseudonymisierung sollte insbesondere dort eingesetzt werden, wo Anonymisierung nicht möglich ist.

Die Qualität der Pseudonymisierungsprozedur hängt von den gleichen Einflußfaktoren ab, wie die Stärke der Anonymisierungsprozedur, nämlich vom Zeitpunkt der Pseudonymisierung, von der Rücknahmefestigkeit der Pseudonymisierungsprozedur, von der Mächtigkeit der Menge, in der sich der Betroffene verbirgt, und von der Verkettungsmöglichkeit von einzelnen Transaktionen/Datensätzen desselben Betroffenen. Insbesondere können Transaktionen/Datensätze, die unter demselben Pseudonym getätigt/gespeichert wurden, miteinander verkettet werden.

Unter gleichen Bedingungen ist die Anonymisierung datenschutzfreundlicher als die Pseudonymisierung. Das Pseudonym kann dazu benutzt werden, den Personenbezug wiederherzustellen. Ansonsten kann ohne Berücksichtigung der genannten Faktoren nicht pauschal beurteilt werden, ob die Anonymisierung oder die Pseudonymisierung datensparsamer ist.

Je nach Verknüpfbarkeit und dem Geheimnisträger des Pseudonyms kann der Personenbezug

- nur vom Betroffenen (selbstgenerierte Pseudonyme),
- nur über eine Referenzliste (Referenz-Pseudonyme) oder
- nur unter Verwendung einer sog. Einweg-Funktion mit geheimen Parametern (Einweg-Pseudonyme)

wiederhergestellt werden.

Pseudonyme ermöglichen es, den Personenbezug herzustellen, so daß die Identität der Person nur in den vorab bestimmten Einzelfällen erkennbar wird.

Pseudonyme sollen zufällig und nicht vorhersagbar gewählt werden. Die Menge der möglichen Pseudonyme soll so mächtig sein, daß bei zufälliger Auswahl nicht zweimal das gleiche Pseudonym generiert wird. Ist eine hohe Sicherheit erforderlich, muß die Menge der Pseudonymkandidaten mindestens so mächtig sein, wie der Wertebereich sicherer kryptografischer Hashfunktionen (siehe Abschnitt „Hashfunktionen“).

Pseudonyme sollten insbesondere nicht anwendungsübergreifend, sondern nur für jeweils ein Verfahren eingesetzt werden. Jede anwendungsübergreifende Benutzung eines einzigen Pseudonyms würde die Gefahr erhöhen, daß aus sämtlichen, mit dem Pseudonym verbundenen Daten ein detailliertes Personenprofil erstellt werden kann, das wiederum den Rückschluß auf eine bestimmte Person erleichert. Aber auch innerhalb einer Anwendung ist die Verwendung nur eines einzigen Pseudonyms nicht unproblematisch.

4.1 Selbstgenerierte Pseudonyme

Selbstgenerierte Pseudonyme werden ausschließlich vom Betroffenen vergeben und nicht mit Identitätsdaten gleichzeitig verwendet oder gespeichert. Somit kann auch der Personenbezug nur vom Betroffenen selbst wiederhergestellt werden, i.d.R. nicht jedoch durch den Betreiber der IuK-Systeme.

Erfüllt die Menge der möglichen Pseudonyme die obigen Kriterien nicht, so ist ein Abgleich der selbstgewählten Pseudonyme mit den schon benutzten notwendig. Dies ist nur akzeptabel, wenn sich im „Trefferfall“ nicht ermitteln läßt, wer das Pseudonym ursprünglich gewählt hat. Kann das für eine Person in Frage kommende Pseudonym vorhergesagt werden, so kann zumindest ermittelt werden, ob Daten zu dieser Person bereits gespeichert sind. Diese Vorhersage dürfte z. B. bei selbstgewählten Vor- und Zunamen oder beim wählbaren Anteil von Autokennzeichen oft funktionieren.

Selbstgenerierte Pseudonyme sollten Verwendung finden bei wissenschaftlichen Studien, die einerseits aggregierte Auskünfte über bestimmte Personengruppen geben sollen, andererseits aber auch den Betroffenen die Möglichkeit einräumen möchten, sich über ihre persönlichen Einzelergebnisse unerkannt zu informieren. Da es für die auswertende Stelle nicht erforderlich ist, die erhobenen Daten personenbezogen auszuwerten, kann statt des Namens ein vom Betroffenen selbstgewähltes Pseudonym verwendet werden, mit dessen Hilfe der Betroffene – und nur er selbst – die Ergebnisse in Erfahrung bringen kann, die ausschließlich seinen Einzelfall betreffen.

4.2 Referenz-Pseudonyme

Bei Referenz-Pseudonymen kann der Personenbezug über entsprechende Referenzlisten wiederhergestellt werden. Ohne Hinzuziehung entsprechender Referenzlisten ist die Identität des Betroffenen i.d.R. jedoch nicht zu ermitteln.

Referenz-Pseudonyme eignen sich für Anwendungen, bei denen der Betroffene nur in bestimmten Ausnahmefällen ermittelt werden muß, beispielsweise bei fehlerhaften Zahlungsvorgängen. Um zu erreichen, daß die Pseudonyme nicht aufgelöst werden, ist es notwendig, die Referenzliste räumlich und organisatorisch getrennt von den pseudonymisierten Datensätzen z. B. in einer Vertrauensstelle (siehe Abschnitt „Vertrauensstellen“) zu speichern. Als besserer Schutz gegen die unbefugte Aufdeckung eines Pseudonyms können die Codes, die in den Referenzlisten zur Wiederherstellung des Personenbezugs gespeichert sind, auch auf mehrere Vertrauensstellen verteilt werden. Nur wenn sämtliche arbeitsteilig operierenden Akteure bereit sind, ihre jeweiligen Referenzlisten zur Verfügung zu stellen, kann das verwendete Pseudonym einer bestimmten Person zugeordnet werden.

4.3 Einweg-Pseudonyme

Einweg-Pseudonyme zeichnen sich dadurch aus, daß sie mittels Einweg-Funktion aus personenbezogenen Identitätsdaten – zumeist auf der Basis asymmetrischer Verschlüsselungsverfahren – gebildet werden. Dabei werden Einweg-Funktionen verwendet, die mit hoher Wahrscheinlichkeit ausschließen, daß die Identitätsdaten zweier Personen auf ein gemeinsames Pseudonym abgebildet werden.

Der Zusammenhang zwischen Identitätsdaten und Pseudonym wird folglich nicht mehr durch eine Tabelle (wie bei Referenzpseudonymen), sondern durch eine explizit formulierte (parametrisierbare) Vorschrift hergestellt. Die Sicherheit sollte nicht auf der Geheimhaltung dieser Vorschrift, sondern auf der Geheimhaltung der Parameter beruhen. Bei Referenzpseudonymen ist statt dessen die Tabelle geheimzuhalten.

Sowohl der Betroffene als auch der Betreiber des Verfahrens können nur dann depseu-donymisieren, wenn sowohl die Parameter bekannt sind als auch die Abbildungsvorschrift bekannt ist/benutzt wird:

- Soll festgestellt werden, zu welcher Person ein bestimmtes Pseudonym zugeordnet ist, muß lediglich mittels der Abbildungsvorschrift aus den Identitätsdaten sämtlicher Personen, aus deren Reihen der Betroffene ermittelt werden soll, das jeweilige Pseudonym gebildet und mit dem zuzuordnenden Pseudonym verglichen werden.
- Andererseits läßt sich ermitteln, ob eine oder mehrere Personen mit einem Pseudonym in einem Datenbestand verzeichnet ist (sind), wenn Identitätsdaten und Abbildungsvorschrift (samt Parameter) bekannt sind. Falls dies zutrifft, sind auch die unter den entsprechenden Pseudonymen gespeicherten Daten zuordenbar.

Der Unterschied zu Referenzpseudonymen besteht darin, daß die Identitätsdaten der Betroffenen in den meisten Anwendungen nicht gespeichert werden müssen. Analog zu den Referenzpseudonymen ist aber auch hier eine Funktionentrennung notwendig: Instanzen, die die Pseudonyme verwalten bzw. die geheimen Parameter

kennen und solche, die nur mit pseudonymisierten Daten umgehen, müssen voneinander getrennt werden. Bei Einhaltung dieser Funktionentrennung erscheinen die pseudonymisierten Identitätsdaten für diejenige Instanz, die nur mit den pseudonymisierten Daten umgehen kann, wie anonymisierte Daten.

Einweg-Pseudonyme eignen sich zum einen für Längsschnittuntersuchungen, bei denen nachträglich erhobene personenbezogene Daten mit Bestandsdaten zusammengeführt werden, ohne daß der Personenbezug für die statistische Auswertung der Daten erforderlich ist. Zum anderen können Einweg-Pseudonyme bei Auskunftssystemen eingesetzt werden, die Auskunft über die Zugehörigkeit bzw. Nicht-Zugehörigkeit einer Person zu einer bestimmten Gruppe geben, ohne daß dabei personenbezogene Identitätsdaten gespeichert werden müssen.

5. Realisierungshilfen

5.1 Hashfunktionen

Hashfunktionen werden in vielfältigem Zusammenhang in Sicherheitsverfahren verwendet, z. B. zur Unterstützung der Authentikation, der Erkennung der Datenunversehrtheit oder dem Urheber- und Empfängernachweis.

Bei einer Hashfunktion handelt es sich um einen Algorithmus, der eine Nachricht (Bitfolge) beliebiger Länge auf eine Nachricht (Bitfolge) fester, kurzer Länge – den sogenannten Hashwert – abbildet. Eine Hashfunktion soll über folgende Eigenschaften verfügen:

- **Einwegfunktions-Eigenschaft,** d. h. zu einem vorgegebenen Wert soll es mit vertretbarem Aufwand unmöglich sein, eine Nachricht zu finden, die eben diesen Wert als Hash-wert hat. Dieser „vertretbare Aufwand“ hängt vom Entwicklungsstand der einsetzbaren Technik und den Sicherheitsanforderungen des Anwenders ab.
- **Kollisionsfreiheit,** d. h. es soll mit vertretbarem Aufwand unmöglich sein, zwei Nachrichten mit demselben Hashwert zu finden.

Bei der Erzeugung von Pseudonymen ist besonders die Kollisionsfreiheit gefordert. Hashfunktionen sind im Gegensatz zu vielen Verschlüsselungsalgorithmen öffentlich bekannt und unterliegen damit intensiven Analysen von Experten, so daß ihre Stärken und Schwächen im allgemeinen bekannt sind. Zu den bekanntesten gehören MD-4, MD-5, SHA-1, RIPEMD und RIPEMD-160. Einige davon haben sich als unbrauchbar zur Erzeugung von Pseudonymen herausgestellt, da sie nicht kollisionsfrei sind. In Europa hat sich RIPEMD-160 als Standard durchgesetzt. RIPEMD-160 ist nach ISO/IEC 10118-3 genormt.

Zur Erzeugung von sicheren Pseudonymen empfiehlt es sich, eine Hashfunktion auszuwählen, die schon länger veröffentlicht und wissenschaftlich untersucht ist. Verschiedene Verfahren sind denkbar, vor Umsetzung ist allerdings unbedingt der Rat von Experten einzuholen.

5.2 Digitale Signaturen

Eine digitale Signatur ist ein mit einem privaten Signaturschlüssel erzeugtes Siegel zu digitalen Daten, das mit Hilfe eines zugehörigen öffentlichen Schlüssels, der mit einem Sig-naturschlüssel-Zertifikat versehen ist, den Inhaber des Signaturschlüssels und die Unverfälschtheit der Daten erkennen läßt [SigG].

Verfahren zur digitalen Signatur sind aus elektronischen Kommunikationssystemen bekannt. Mit der digitalen Signatur kann der Nachweis der Urheberschaft eines Objektes (z. B. eines digitalen Schriftstücks wie einer E-Mail (elektronische Post)) erbracht werden. Ein direkter Rückschluß auf denjenigen, der das Objekt signierte, ist möglich – ja gewollt. Da die digitale Signatur (u.a. durch Anwendung von Hashfunktionen) jeweils speziell über dem zu signierenden Objekt gebildet wird, ist damit gleichzeitig die Integrität des signierten Objekts nachprüfbar.

Erzeugt der Betroffene selbst dezentral die Schlüssel, handelt es sich in gewisser Weise um ein spezielles selbstgeneriertes Pseudonym, weil der spezielle (private) Signaturschlüssel (zur Erzeugung der digitalen Signatur) nur dem rechtmäßigen Benutzer bekannt und zugänglich ist.

5.3 (Signaturschlüssel-)Zertifikat

Ein Zertifikat ist eine mit einer digitalen Signatur versehene digitale Bescheinigung über die Zuordnung eines öffentlichen Signaturschlüssels zu einer natürlichen Person [SigG]. Dabei handelt es sich um ein spezielles selbstgeneriertes Pseudonym der das Zertifikat ausstellenden Institution, mit dem die Zuordenbarkeit zweier, voneinander abhängiger Pseudonyme zu einer Person (öffentlicher Signaturschlüssel und zugehöriger privater Signaturschlüssel) sichergestellt wird.

5.4 Blinde digitale Signatur

Eine „blinde digitale Signatur“ stellt eine Variante der digitalen Signatur dar, mit der die Anonymität des Benutzers gewahrt wird. Der Unterschied zwischen beiden Signaturformen besteht darin, daß bei der blinden digitalen Signatur kein Rückschluß auf denjenigen möglich ist, der das signierte Objekt verwendet (Beispiel: eine Banknote entspricht einem blind digital signierten Objekt; der Benutzer der Banknote bleibt anonym). Die Echtheit des Objektes wird von einem außenstehenden Dritten durch seine digitale Signatur bestätigt (Zertifikat), der Benutzer tritt mit seiner eigenen Identität nicht in Erscheinung. Diese Form der digitalen Signatur wird z. B. für „Ecash“ verwendet.

5.5 Biometrische Verfahren

Bei der biometrischen Verschlüsselung werden körperliche Merkmale wie Augennetzhaut, Fingerabdruck, usw. z. B. durch optische Geräte oder besondere Chipkarten derart digitalisiert und zu einer digitalen Zeichenfolge aufbereitet, daß diese als eindeutiges Merkmal für die

betreffende Person verwendet werden können. Zur Feststellung von Identität und Authentizität der Person als Benutzer eines IuK-Systems ist das betreffende körperliche Merkmal erneut zu digitalisieren und mit dem gespeicherten Muster zu vergleichen. Der Berechnungsvorgang zur Erzeugung dieser identifizierenden Zeichenfolge ist nicht umkehrbar, er stellt eine Einwegfunktion dar. Insoweit ist ein derart erzeugtes biometrisches Merkmal einem Einweg-Pseudonym gleichzusetzen.

5.6 *Vertrauensstellen*

Vertrauensstellen sind für die Realisierung bestimmter Sicherheitsdienste und für die Akzeptanz ganzer IT-Infrastrukturen erforderlich. Die Funktion einer solchen Vertrauensstelle wird oft mit der eines Notars, also einer neutralen, unbeteiligten Instanz, verglichen. Dieser Instanz müssen in der Regel alle Beteiligten (das sind der Benutzer und ggf. seine Kommunikations- und Geschäftspartner sowie ggf. die Betreiber der verwendeten IuK-Systeme) im Hinblick darauf vertrauen, daß sie ihre Aufgaben korrekt erfüllt.

Der Benutzer vertraut beispielsweise darauf, daß die Geheimhaltung seiner wahren Identität bei Verwendung eines Pseudonyms gewährleistet wird bzw. daß – wenn rechtmäßig seine Identität aufgedeckt wird – er unverzüglich informiert wird, wann, gegenüber wem und warum die Aufdeckung erfolgte.

Das Vertrauen des Betreibers eines IuK-Systems erstreckt sich darauf, daß zur Wahrung seiner legitimen Interessen im definierten und vereinbarten Bedarfsfall (z. B. Aufdeckung von Leistungsmißbrauch) die tatsächliche Identität des Benutzers offengelegt wird.

Aufgaben von Vertrauensstellen können, neben den kommerziellen oder öffentlichen Trust Center als sogenannte Trusted Third Parties (TTPs), auch unter der Kontrolle des Benutzers arbeitende Personal Trust Center (PTCs) übernehmen, z. B. „intelligente“ Sicherheitstoken wie SmartCards. Man unterscheidet vier Aufgabenbereiche, die von Vertrauensstellen erfüllt werden *können*:

- **Schlüsselmanagement**
  - Schlüsselgenerierung und -zurücknahme
  - Speicherung von (öffentlichen) Schlüsseln
  - Verteilung und Löschung/Sperrung von Schlüsseln
- **Beglaubigungsleistungen**
  - Ausstellung von Zertifikaten für öffentliche Schlüssel
  - Personalisierung von Schlüsseln: Zuordnung zu einem Benutzer (Identität oder Pseudonym)
  - Registrierung von Benutzern (Identitätsbeglaubigung und ggf. Zuordnung zu Pseudonymen)
  - Personalisierung von PTCs
  - Zertifizierung/Zulassung von TTPs
- **Treuhänderfunktion**

  treuhänderisches Hinterlegen beispielsweise von
  - personenbezogenen Daten, z. B. Identifikationsdaten
  - Schlüsseln zur Datensicherung
- **Serverfunktionen**

  Online-Bereitstellung von Informationen für die Sicherheitsinfrastruktur, z. B.
  - Verzeichnisse von (öffentlichen) Benutzerschlüsseln
  - Authentisierungsinformationen (z. B. bei Kerberos)
  - Zeitstempel
  - Warnungen bei kritischen Sicherheitsereignissen

Um eine größtmögliche Vertrauenswürdigkeit der Vertrauensstellen zu erreichen, ist ein hohes Maß an Zuverlässigkeit und Fachkunde erforderlich. Die geforderte Neutralität und Unabhängigkeit einer Vertrauensstelle darf nicht durch Interessenkollisionen eingeschränkt oder gefährdet werden; solche Probleme können durch ungeeignete Kombinationen mehrerer der oben genannten (Teil-)Aufgaben bzw. Rollen entstehen. Darüber hinaus sollten Aufgaben mit besonderen Sicherheitsanforderungen nicht von einer einzigen Vertrauensstelle erledigt, sondern auf mehrere Stellen verteilt werden. Außerdem sollten die Vertrauensstellen nach einer veröffentlichten Policy arbeiten, die eine klare Darstellung der Aufgaben und Sicherheitsanforderungen umfaßt und die möglichst benutzerüberprüfbar realisiert ist.

Nicht alle der o.a. Aufgaben von Trust Center sind zur Datenvermeidung und damit zur verstärkten Wahrung der Privatheit des Einzelnen geeignet, wie z. B. insbesondere die Generierung von Schlüsseln in Vertrauensstellen und das Bereithalten von öffentlichen Schlüsseln mit Identitäten.

Als Beispiele für Vertrauensstellen können hier die Funktionalität von First Virtual (siehe Anlage, Abschnitt „Elektronische Zahlungssysteme“) sowie die im Signaturgesetz [SigG] beschriebenen Zertifizierungsstellen für die öffentlichen Schlüssel im Rahmen der digitalen Signatur genannt werden.

Im übrigen gibt es mittlerweile bereits eine Reihe von Unternehmen in der Bundesrepublik Deutschland, die einige oder alle der o.a. Dienstleistungen kommerziell anbieten.

5.7 *Der Identity Protector*

Wie oben dargestellt, lassen sich IuK-Systeme, für die eine anonyme Nutzungsform nicht vollständig möglich ist, derart in unterschiedliche Einzelprozesse zerlegen, daß unmittelbar personenbezogene Daten (Identitätsdaten) nur erhoben, gespeichert und verarbeitet werden, wo dies unabdingbar nötig ist.

Durch geeignete technische Maßnahmen muß dafür Sorge getragen werden, daß die Bereiche des IuK-Systems,

die den vollen Personenbezug mit den Identitätsdaten benötigen, strikt von jenen getrennt werden, die nur mit einem Pseudonym auskommen. D.h. nur die tatsächlich und unmittelbar benötigten Daten stehen dem jeweiligen Prozeß zur Verfügung. Eine Zusammenführung von Identitätsdaten und Pseudonymdaten ist nur unter vorab und genau definierten Umständen möglich.

Diese Aufgaben kann ein „Identity Protector“ leisten. Er kann als Systemelement (Prozeß) betrachtet werden, das den Austausch von Identitätsdaten und Pseudonymdaten zwischen den übrigen Systemelementen steuert.

Für einen „Identity Protector“ sind verschiedene Ausprägungsformen möglich:

a) eigenständiges Element in einem IuK-System

b) eigenständiges IuK-System, das unter der Kontrolle des Benutzers steht

c) eigenständiges IuK-System, das unter der Kontrolle einer Vertrauensstelle steht (siehe Unterabschnitt „Vertrauensstellen“)

Im Falle a) sollte der Identity Protector ein – auch für den Betreiber des IuK-Systems – unveränderbarer Baustein sein. Die Realisierung ließe sich als Softwarebaustein im IuK-System selbst, im zugrundeliegenden Betriebssystem oder auch als Hardwarekomponente mit zugehöriger Software (z. B. als „Black-Box-Lösung“) bewerkstelligen.

Im Falle b) wäre eine Abbildung des Identity Protectors z. B. in Form einer Smart-Card als intelligentes Sicherheitstoken und als PTC möglich.

Der Identity Protector kann folgende Funktionalitäten leisten:

- kontrollierte Offenlegung und Freigabe der Identität
- Generierung von Pseudonymen
- Umsetzung von Pseudonymen in weitere Pseudonyme
- Umsetzung von Identitäten in Pseudonyme (Pseudonymisierung)
- Umsetzung von Pseudonymen in Identitäten (Depseudonymisierung)
- vorbeugende Mißbrauchsbekämpfung (u.a. durch die erstgenannte Funktionalität)

Zur Realisierung eines Identity Protectors stehen alle oben genannten Hilfsmittel zur Verfügung. Nicht alle diese Techniken müssen aber für jede Ausprägung eines Identity Protectors verwendet werden.

Die Funktionstüchtigkeit und Unveränderbarkeit des Identity Protectors müßte konsequenterweise mittels Zertifizierung und (kryptografischer) Versiegelung durch eine unabhängige Vertrauensstelle sichergestellt werden.

6. Zusammenfassung und Handlungsempfehlung

Datenvermeidung und Datensparsamkeit spielen in der Anwendung der IuK-Technologie bisher nur eine untergeordnete Rolle. Um zukünftig den Ansprüchen an Datenschutzfreundlichkeit gerecht zu werden, muß das Streben nach Datensparsamkeit die Entwicklung und den Betrieb von IuK-Systemen genauso beeinflussen, wie die Forderung nach Datensicherheit.

Für die Akzeptanz von Multimedia wird die Sicherstellung des Datenschutzes und der Privatheit des Einzelnen von entscheidender Bedeutung sein. Es ist absehbar, daß in Zukunft Produkte und Dienstangebote bei im übrigen gleicher Qualität und gleichem Preis Wettbewerbsvorteile haben werden, wenn sie datenschutzfreundlicher als die anderen sind. Ein Produkt oder Dienstangebot, das mit möglichst wenig personenbezogenen Daten seiner Nutzer auskommt, wird dem anderen vorgezogen, das umfangreiche Datenspuren erzeugt.

Die Datenschutzbeauftragten des Bundes und der Länder wollen diesen Prozeß beschleunigen und in Zusammenarbeit mit Herstellern und Anbietern auf datenschutzgerechte Lösungen hinarbeiten.

Neue Informations- und Kommunikationssysteme sollten folgende **Grundsätze** beachten:

- IuK-Systeme sollten so gestaltet werden, daß keine personenbezogenen Daten erhoben, gespeichert und verarbeitet werden, d. h. daß eine anonyme Nutzung möglich ist.
- In den Systemteilbereichen, in denen für einen definierten Zeitraum personenbezogene Daten für die spezifische Funktionalität unabdingbar sind, sollte festgelegt werden, ob und wann eine Anonymisierung, oder falls dies nicht möglich ist, eine Pseudonymisierung erfolgen kann.

Um diese Grundsätze bei der Entwicklung oder Modifizierung von IuK-Systemen in ausreichendem Maße berücksichtigen zu können, ist folgende **Vorgehensweise** empfehlenswert:

Zunächst müssen datenverarbeitende Systeme und Teilsysteme einschließlich ihrer Schnittstellen definiert werden. Bei dieser Definition muß auch eine Unterscheidung derjenigen Systeme und Teilsysteme erfolgen, in denen

1. ohne personenbezogene Daten gearbeitet werden kann,
2. personenbezogene Daten anonymisiert werden können,
3. personenbezogene Daten pseudonymisiert werden können bzw.
4. der direkt herstellbare Personenbezug unvermeidlich ist.

Ist eine Anonymisierung oder eine Pseudonymisierung erforderlich, so ist für das jeweilige System/Teilsystem eine entsprechende Prozedur zu finden,

- die die personenbezogenen Daten frühestmöglich anonymisiert bzw. pseudonymisiert,
- die nicht unzulässig beeinflußt (Integrität) werden kann,

- die aus dem System/Teilsystem nicht mit geringem Aufwand wieder entfernt werden kann (Rücknahmefestigkeit),
- die den Betroffenen in einer hinreichend großen Menge möglicher Betroffener verbirgt und
- die die Verkettbarkeit von Einzeldaten oder Transaktionen zu Datenspuren unterdrückt.

Stellt sich heraus, daß die vorhandenen Risiken mit dem so konstruierten System nicht hinreichend reduziert werden können, so müssen ggf. Teile des Definitionsprozesses und Teile des Gestaltungsprozesses wiederholt werden.

Bereits heute ist eine Reihe von Technologien und Hilfsmittel zur Erreichung von verbessertem Datenschutz durch Technik verfügbar. Die Technologie, die dafür gesorgt hat, daß personenbezogene Daten gespeichert, genutzt und weitergegeben werden können, ist auch zur Wahrung der Privatheit des Einzelnen nutzbar. Diese Möglichkeiten der modernen Datenschutztechnologie, die mit dem Begriff **„Privacy enhancing technology (PET)“** eine Philosophie der Datenvermeidung und der Datensparsamkeit beschreibt und ein ganzes System technischer Maßnahmen umfaßt, sollten genutzt werden.

Verbraucher sollten durch gezielte Nachfrage die Verwendung datenschutzfreundlicher Technologien in IuK-Systemen fordern und fördern.

Auch der Gesetzgeber muß die Verwendung datenschutzfreundlicher Technologien fordern und fördern.

An Industrie und Dienstleistungsanbieter ergeht der Appell, für den Verbraucher transparentere Systeme zu schaffen und datenschutzfreundliche Technologien verstärkt in ihre Systeme einzubauen.

Anlage 28 (zu Nr. 2.4)

Commission de la
Protection de la Vie Privée
c/o Ministère de la Justice
Mr. Paul Thomas
Président
Bd. de Waterloo, 115
B-1000 Bruxelles
BELGIEN

Registertilsynet
– President –
Mr. Henrik Waaben
Christians Brygge 28 4 sal
DK-1559 Kobenhavn V
DÄNEMARK

Data Protection Ombudsman
Mr. Reijo Aarnio
Albertinkatu 25, 3. krs
P.O.Box 315
SF-00181 Helsinki
FINNLAND

Commission Nationale de
l' Informatique et des Libertés
M. le Président Michel Gentot
21, rue Saint Guillaume
F-75340 Paris Cedex 07
FRANKREICH

Data Protection Commission
The President
Mr. K. Dafermos
Omirou St. 8
GR –10564 Athens
GRIECHENLAND

Data Protection Registrar
Ms. Elizabeth France
Wycliffe House, Water Lane,
GB-Wilmslow, Cheshire SK9 5AS
GROSSBRITANNIEN

Garante per la protezione dei
dati personali
Segretario generale
Mr. Chairman Stefano Rodotà
Via della Chiesa Nuova, 8
I-00186 Roma
ITALIEN

Data Protection Commissioner
c/o Department of Justice
Mr. Fergus Glavey
Block 4, Irish Life Centre
Talbot Street
IRL-Dublin 1
IRLAND

Secrétaire de la Commission
à la Protection des données nominatives
Mr. René Faber
Ministère de la Justice
16 Bd. Royal
L-2934 Luxembourg
LUXEMBURG

Registratiekamer
– President –
Mr. Peter Hustinx
Postbus 93374
NL-2509 AJ The Hague
NIEDERLANDE

Datenschutzkommisson
Dr. Waltraud Kotschy
Bundeshaus
Ballhausplatz 1
A-1014 Wien
ÖSTERREICH

President of the Portuguese
Data Protection Commission
Mr. Augusto Victor Coelho
Rua de S. Bento, 148-3°
P-1200 Lisboa
PORTUGAL

Datainspektionen
Mr. Director General
Ulf Widebäck
Box 8114
S-10420 Stockholm
SCHWEDEN

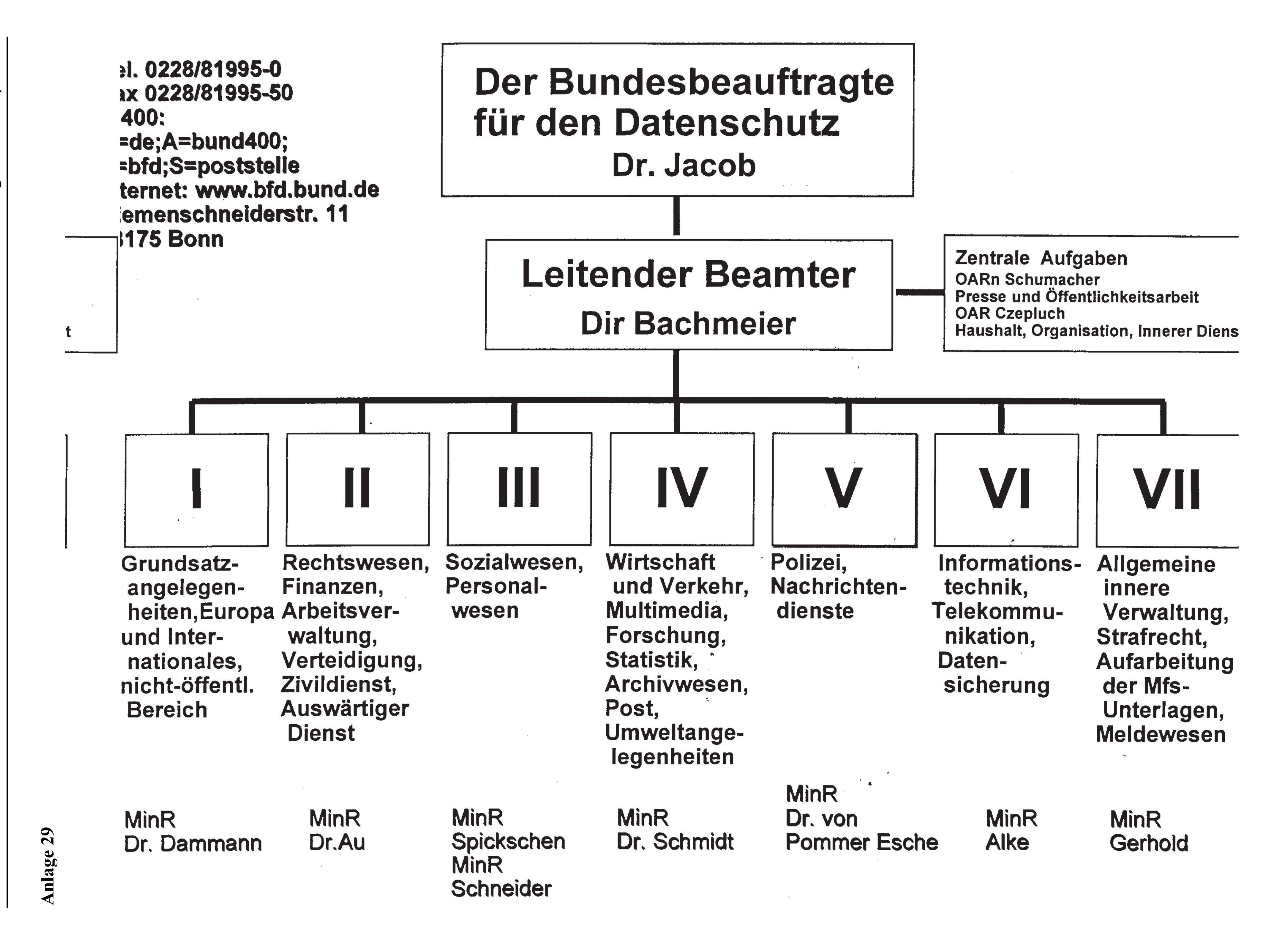
Director de la Agencia de Protección de
Datos
Mr. Juan Manuel Fernández Lopéz
Paseo de la Castellana
41-5ª planta
E-28046 Madrid
SPANIEN

n a c h r i c h t l i c h :

Icelandic Data Protection Commissioner
Mr. Thorgeir Orlygsson
Arniarhvoll
ICELAND-150 Reykjavik
ISLAND

Datatilsynet
Director General
Mr. Georg Apenes
Berhard-Getz-Gt. 2
P.B. 8177 DEP 0034
N-Oslo 1
NORWEGEN

Anlage 29



Der Bundesbeauftragte
für den Datenschutz
Dr. Jacob
el. 0228/81995-0
ax 0228/81995-50
400:
=de;A=bund400;
=bfd;S=poststelle
ternet: www.bfd.bund.de
emenschneiderstr. 11
175 Bonn
t
Leitender Beamter
Dir Bachmeier
Zentrale Aufgaben
OARn Schumacher
Presse und Öffentlichkeitsarbeit
OAR Czepluch
Haushalt, Organisation, Innerer Diens
I
Grundsatz-
angelegen-
heiten,Europa
und Inter-
nationales,
nicht-öffentl.
Bereich
MinR
Dr. Dammann
II
Rechtswesen,
Finanzen,
Arbeitsver-
waltung,
Verteidigung,
Zivildienst,
Auswärtiger
Dienst
MinR
Dr.Au
III
Sozialwesen,
Personal-
wesen
MinR
Spickschen
MinR
Schneider
IV
Wirtschaft
und Verkehr,
Multimedia,
Forschung,
Statistik,
Archivwesen,
Post,
Umweltange-
legenheiten
MinR
Dr. Schmidt
V
Polizei,
Nachrichten-
dienste
MinR
Dr. von
Pommer Esche
VI
Informations-
technik,
Telekommu-
nikation,
Daten-
sicherung
MinR
Alke
VII
Allgemeine
innere
Verwaltung,
Strafrecht,
Aufarbeitung
der Mfs-
Unterlagen,
Meldewesen
MinR
Gerhold

Sachregister

Abkürzungsverzeichnis

AA	Auswärtiges Amt
ABl.EG	Amtsblatt der Europäischen Gemeinschaften
AFIS	Automatisiertes Fingerabdruck-Identifizierungssystem
AG	Aktiengesellschaft; aber auch: Arbeitsgruppe
AGB	Allgemeine Geschäftsbedingungen
AK II	Arbeitskreis II „Innere Sicherheit“ der IMK
AK Technik	Arbeitskreis „Technische und organisatorische Datenschutzfragen“
AO	Abgabenordnung
APC	Arbeitsplatzcomputer
AZR-VV	Allgemeine Verwaltungsvorschrift zum AZR-Gesetz und zur AZRG-Durchführungsverordnung
ASYLON	Asyl-online
AsylVfG	Asylverfahrensgesetz
AtG	Atomgesetz
AuslG	Ausländergesetz
AZR	Ausländerzentralregister
AZR-Gesetz	Ausländerzentralregister-Gesetz
AZRG-DV	Verordnung zur Durchführung des Ausländerzentralregistergesetzes
BA	Bundesanstalt für Arbeit
BAfAM	Bundesanstalt für Arbeitsschutz und Arbeitsmedizin
BAFl	Bundesamt für die Anerkennung ausländischer Flüchtlinge
BAföG	Bundesausbildungsförderungsgesetz
BAG	Bundesamt für Güterverkehr
BAV	Bundesaufsichtsamt für das Versicherungswesen
BAZ	Bundesamt für den Zivildienst
BBG	Bundesbeamtengesetz
BDO	Bundesdisziplinarordnung
BDSG	Bundesdatenschutzgesetz
BEK	Barmer Ersatzkasse
BfA	Bundesversicherungsanstalt für Angestellte
BfD	Bundesbeauftragter für den Datenschutz
BfF	Bundesamt für Finanzen
BfV	Bundesamt für Verfassungsschutz
BG	Berufsgenossenschaft
BGB	Bürgerliches Gesetzbuch
BGBl.	Bundesgesetzblatt
BGHSt	Entscheidungen des Bundesgerichtshofes in Strafsachen
BGS	Bundesgrenzschutz
BGSG	Bundesgrenzschutzgesetz
Bit	Binary Digit
BK	Bundeskanzleramt
BKA	Bundeskriminalamt
BKAG	Gesetz über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten
BKK	Betriebskrankenkasse
BMA	Bundesministerium für Arbeit und Sozialordnung
BMBF	Bundesministerium für Bildung und Forschung
BMF	Bundesministerium der Finanzen
BMG	Bundesministerium für Gesundheit
BMI	Bundesministerium des Innern
BMJ	Bundesministerium der Justiz
BMPT	Bundesministerium für Post und Telekommunikation
BMVBW	Bundesministerium für Verkehr, Bau- und Wohnungswesen
BMVg	Bundesministerium der Verteidigung
BMWi	Bundesministerium für Wirtschaft und Technologie
BND	Bundesnachrichtendienst
BNDG	Gesetz über den Bundesnachrichtendienst

BPersVG Bundespersonalvertretungsgesetz
BPräsA Bundespräsidialamt
BR-Drs. Bundesrats-Drucksache
BSHG Bundessozialhilfegesetz
BSI Bundesamt für Sicherheit in der Informationstechnik
BStatG Bundesstatistikgesetz
BStBl Bundessteuerblatt
BStU Bundesbeauftragter für die Unterlagen des Staatssicherheitsdienstes der ehemaligen DDR
BT-Drs. Bundestags-Drucksache
BVA Bundesverwaltungsamt
BVerfG Bundesverfassungsgericht
BVerfGE Entscheidungen des Bundesverfassungsgerichts
BVerfSchG Bundesverfassungsschutzgesetz
BVerfSchGE Bundesverfassungsschutzgesetz-Entwurf
BVerwG Bundesverwaltungsgericht
BVFG Bundesvertriebenengesetz
BZR Bundeszentralregister
BZRG Bundeszentralregistergesetz

C.SIS technische Unterstützungseinheit des Schengener Informationssystems
CCIVBB Competence Center Informationsverbund Berlin-Bonn
CD-ROM Compact Disc – Read Only Memory
CIS Zollinformationssystem (Customs Information System)
CLIP Calling Line Identification Presentation
CNIL Commission Nationale de l’Informatique et des Libertés

d.h. das heißt
DAK Deutsche Angestellten-Krankenkasse
DDR Deutsche Demokratische Republik
DFS Deutsche Flugsicherungs GmbH
DNA Desoxyribonuclein acid (acid = Säure)
DRK Deutsches Rotes Kreuz
DSB Datenschutzbeauftragter
DSK Datenschutzkapitel
DTAG Deutsche Telekom AG
DV/dv Datenverarbeitung

E-Mail Electronic Mail
ECU European Currency Unit (Europäische Währungseinheit)
EDS Europäische Drogenstelle
EG Europäische Gemeinschaft
EGV Vertrag zur Gründung der Europäischen Gemeinschaft
EheSchlRG Gesetz zur Neuordnung des Eheschließungsrechts
EPR Elektronisches Personenregister
EStG Einkommensteuergesetz
EU Europäische Union
EUCARIS Europäisches Fahrzeug- und Führerschein-Informationssystem
EuGH Europäischer Gerichtshof
EUROCONTROL Europäische Organisation für Flugsicherung
EURODAC Europäisches daktyloskopisches Fingerabdrucksystem zur Identifizierung von Asylbewerbern
EUROPOL Zentrales Europäisches Kriminalpolizeiamt
EUROSTAT Statistisches Amt der Europäischen Gemeinschaft
EU-Vertrag Vertrag über die Europäische Union
EVN Einzelverbindungsnachweis
EWG Europäische Wirtschaftsgemeinschaft
EWR Europäischer Wirtschaftsraum

FAG Fernmeldeanlagengesetz
FeV Fahrerlaubnis-Verordnung
FKTO Fernmeldekontonummer
FRV Fahrzeugregisterverordnung
FÜV Fernmelde-Überwachungs-Verordnung

G10 Gesetz zu Artikel 10 GG

GBA	Generalbundesanwalt beim Bundesgerichtshof
GG	Grundgesetz
ggf.	gegebenenfalls
GK	Gemeinsame Kontrollinstanz
GwG	Geldwäschegesetz
HFR	Höchstrichterliche Finanzrechtsprechung
HPC	Health Professional Card
HVBG	Hauptverband der gewerblichen Berufsgenossenschaften
i.d.R.	in der Regel
i.S.	im Sinne
i.S.d.	im Sinne des (der)
i.V.m.	in Verbindung mit
ICD-10	International Classification of Diseases – 10th Revision
IMK	Innenministerkonferenz
IMSI	International Mobile Subscriber Identity
INA	IT-gestütztes Nach- und Rücksendeverfahren
INPOL	Informationssystem der Polizei
InVeKoS	Integriertes Verwaltungs- und Kontrollsystem
INZOLL	Informationssystem für den Zollfahndungsdienst
ISDN	Integrated Services Digital Network
IT	Informationstechnik
ITSEC	Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik
IuKDG	Informations- und Kommunikationsdienstegesetz
IuKTechnik	Informations- und Kommunikations-Technik
IVBB	Informationsverbund Berlin-Bonn
JuMiG	Justizmitteilungsgesetz
JVA	Justizvollzugsanstalt
KAN	Kriminalaktennachweis
KBA	Kraftfahrt-Bundesamt
Kbit/s	Kilobit pro Sekunde
KBSt	Koordinierungs- und Beratungsstelle der Bundesregierung für Infromationstechnik in der Bundesverwaltung
Kbyte	Kilobyte
KDV	Kriegsdienstverweigerung
KISLS	Kommunikations- und Informationssystem Luftsicherheit
KPS-Richtlinien	Richtlinien für die Führung kriminalpolizeilicher personenbezogener Sammlungen
KSD/IA	Koordinierungsstelle Schengen/Dublin – Internationale Aufgaben
KVK	Krankenversicherungskarte
LAN	Local Area Network
LBA	Luftfahrt-Bundesamt
LfD	Landesbeauftragter für den Datenschutz
lit.	littera (Buchstabe)
LuftVG	Luftverkehrsgesetz
MAD	Militärischer Abschirmdienst
MADG	Gesetz über den MAD
m.E.	meines Erachtens
MDStV	Mediendienste-Staatsvertrag
MfS	Ministerium für Staatssicherheit/Amt für nationale Sicherheit (der ehemaligen DDR)
MiStra	Mitteilungen in Strafsachen
MiZi	Mitteilungen in Zivilsachen
MOE-Staaten	mittel- und osteuropäische Staaten
Mrd.	Milliarden
MRRG	Melderechtsrahmengesetz
n.F.	neue Fassung
N.SIS	Nationaler Bestand des Schengener Informationssystems
NADIS	Nachrichtendienstliches Informationssystem
NADIS-PZD	Personenzentraldatei im NADIS
NJW	Neue Juristische Wochenschrift

OECD	Organisation für wirtschaftliche Zusammenarbeit und Entwicklung
OFD	Oberfinanzdirektion
OVG	Oberverwaltungsgericht
P3P	Platform for Privacy Preferences
PC	Personalcomputer
PDSV	Postdienstunternehmen-Datenschutzverordnung
PET	Privacy Enhancing Technologies
PIN	persönliche Identifikationsnummer
PK	Personenkennzeichen
PostG	Postgesetz
PStÄndG	Gesetz zur Änderung des Personenstandsgesetzes
PStG	Personenstandsgesetz
PTC	Personal Trust Center
PTRegG	Gesetz über die Regulierung der Telekommunikation und des Postwesens
PZD	Personenzentraldatei
RAF	Rote Armee Fraktion (terroristische Vereinigung)
rd.	rund
RegTP	Regulierungsbehörde für Telekommunikation und Post
RVO	Reichsversicherungsordnung
s.o.	siehe oben
s.u.	siehe unten
Schufa	Schutzgemeinschaft für allgemeine Kreditsicherung
SDAG	Sowjetisch-Deutsche Aktiengesellschaft
SDÜ	Schengener Durchführungsübereinkommen
SGB	Sozialgesetzbuch
SGB I	Sozialgesetzbuch Erstes Buch (Allgemeiner Teil)
SGB III	Sozialgesetzbuch Drittes Buch (Arbeitsförderung)
SGB IV	Sozialgesetzbuch Viertes Buch (Gemeinsame Vorschriften für die Sozialversicherung)
SGB V	Sozialgesetzbuch Fünftes Buch (Gesetzliche Krankenversicherung)
SGB VI	Sozialgesetzbuch Sechstes Buch (Gesetzliche Rentenversicherung)
SGB VII	Sozialgesetzbuch Siebentes Buch (Gesetzliche Unfallversicherung)
SGB X	Sozialgesetzbuch Zehntes Buch (Verwaltungsverfahren)
SGB XI	Sozialgesetzbuch Elftes Buch (soziale Pflegeversicherung)
SigG	Signaturgesetz
SigV	Signaturverordnung
SIM	Subscriber Identity Module
SIS	Schengener Informationssystem
SPAM	Specially Prepared Assented Meat (im Internet Synonym für unerwünschte oder minderwertige Textbeiträge – insbesondere Werbung per E-Mail)
StGB	Strafgesetzbuch
StPO	Strafprozeßordnung
StUG	Gesetz über die Unterlagen des Staatssicherheitsdienstes der ehemaligen Deutschen Demokratischen Republik (Stasi-Unterlagen-Gesetz)
StVÄG	Strafverfahrensänderungsgesetz
StVG	Straßenverkehrsgesetz
SÜG	Sicherheitsüberprüfungsgesetz
TB	Tätigkeitsbericht
TDDSG	Teledienstedatenschutzgesetz
TDG	Teledienstegesetz
TDSV	Telekommunikationsdienstunternehmen-Datenschutzverordnung
TFG	Transfusionsgesetz
TK	Telekommunikation
TK-Anlage	Telekommunikationsanlage
TKG	Telekommunikationsgesetz
TKÜV	Telekommunikations-Überwachungsverordnung (Entwurf)
TKV	Telekommunikations-Kundenschutzverordnung
TPG	Transplantationsgesetz
TTP	Trusted Third Party
u.a.	unter anderem

Ü 1	einfache Sicherheitsüberprüfung
Ü 2	erweiterte Sicherheitsüberprüfung
Ü 3	erweiterte Sicherheitsüberprüfung mit Sicherheitsermittlungen
u.U.	unter Umständen
UCLAF	Unité pour la coordination de la Lutte Antifraude (Betrugsbekämpfungseinheit der Europäischen Kommission)
UNHCR	Hoher Flüchtlingskommissar der Vereinten Nationen
URL	Uniform Resource Locator
usw.	und so weiter
VDR	Verband Deutscher Rentenversicherungsträger
VGH	Verwaltungsgerichtshof
VPOB	Vorprüfungsordnung Bund
VT-BS	Vertriebsteams für Behörden mit Sicherheitsaufgaben
VwGO	Verwaltungsgerichtsordnung
VwZG	Verwaltungszustellungsgesetz
VZ	Volkszählung
VZR	Verkehrszentralregister
WWW	World Wide Web
z.B.	zum Beispiel
z.T.	zum Teil
z.Z.	zur Zeit
ZDG	Zivildienstgesetz
ZEVIS	Zentrales Verkehrsinformationssystem
ZFER	Zentrales Fahrerlaubnisregister
ZIS	Zollinformationssystem
ZKA	Zentraler Kreditausschuß
ZKA	Zollkriminalamt
ZStV	Zentrales Staatsanwaltschaftliches Verfahrensregister

Tätigkeitsbericht	Zeitraum	Bundestags-Drucksache
1.	1978	8/2460
2.	1979	8/3570
3.	1980	9/93
4.	1981	9/1243
5.	1982	9/2386
6.	1983	10/877
7.	1984	10/2777
8.	1985	10/4690
9.	1986	10/6816
10.	1987	11/1693
11.	1988	11/3932
12.	1989	11/6458
13.	1990	12/553
14.	1991 – 1992	12/4805
15.	1993 – 1994	13/1150
16.	1995 – 1996	13/7500

Druck: Bonner Universitäts-Buchdruckerei, 53113 Bonn
Vertrieb: Bundesanzeiger Verlagsgesellschaft mbH, Postfach 13 20, 53003 Bonn, Telefon: 02 28/3 82 08 40, Telefax: 02 28/3 82 08 44
ISSN 0722-8333